

Public Document Pack

Blackpool Council

21 June 2016

To: Councillors Benson, Cox, Galley, Hobson, Hunter, Matthews, O'Hara, Owen and Roberts

The above members are requested to attend the:

AUDIT COMMITTEE

Thursday, 30 June 2016 at 6.00 pm
in Committee Room B, Town Hall, Blackpool

A G E N D A

1 DECLARATIONS OF INTEREST

Members are asked to declare any interests in the items under consideration and in doing so state:

- (1) the type of interest concerned; and
- (2) the nature of the interest concerned

If any member requires advice on declarations of interests, they are advised to contact the Head of Democratic Governance in advance of the meeting.

2 MINUTES OF THE LAST MEETING HELD ON 26 MAY 2016 (Pages 1 - 8)

To agree the minutes of the last meeting of the Audit Committee held on 26 May 2016 as a true and correct record.

3 LIGHTPOOL PROJECT - INTERNAL AUDIT (Pages 9 - 22)

To provide an update on actions taken to address the recommendations of the Internal Audit review on the Lightpool project dated 11 February 2016.

4 STRATEGIC RISK REGISTER - INABILITY TO RESPOND TO A MAJOR INCIDENT (Pages 23 - 26)

To consider a progress report on individual risks identified in the Council's Strategic Risk Register.

- 5 ANNUAL GOVERNANCE STATEMENT 2015/2016** (Pages 27 - 44)
- To consider the Annual Governance Statement for 2015/2016.
- 6 KPMG TECHNICAL UPDATE** (Pages 45 - 70)
- To consider KPMG's report providing an overview on progress in delivering its responsibilities as the external auditors.
- 7 STRATEGIC RISK REGISTER** (Pages 71 - 82)
- To consider the Council's revised Strategic Risk Register.
- 8 AUDIT COMMITTEE SELF-EVALUATION** (Pages 83 - 90)
- To consider the feedback from the self-evaluation exercise undertaken by the Audit Committee and senior officers who engage with the Committee on a regular basis.
- 9 REGULATION OF INVESTIGATORY POWERS ACT (2000) POLICY AND PROCEDURE** (Pages 91 - 390)
- To consider the Regulation of Investigatory Powers Act (2000) (RIPA) policy and procedure.
- 10 DATE OF NEXT MEETING**
- To note the date and time of the next meeting of the Committee as 22 September 2016, commencing at 6pm.

Venue information:

First floor meeting room (lift available), accessible toilets (ground floor), no-smoking building.

Other information:

For queries regarding this agenda please contact Chris Kelly, Senior Democratic Governance Adviser, Tel: 01253 477164, e-mail chris.kelly@blackpool.gov.uk

Copies of agendas and minutes of Council and committee meetings are available on the Council's website at www.blackpool.gov.uk.

Present:

Councillor Galley (in the Chair)

Councillors

Hobson	O'Hara	Roberts	Scott
Matthews	Owen	Ryan	Singleton

In Attendance:

Mr Neil Jack, Chief Executive

Mr Steve Thompson, Director of Resources

Mr Mark Towers, Director of Governance and Partnerships

Ms Tracy Greenhalgh, Chief Internal Auditor

Mr Iain Leviston, Manager, KPMG

Mr Chris Kelly, Senior Democratic Governance Adviser (Scrutiny)

1 DECLARATIONS OF INTEREST

There were no declarations of interest on this occasion.

2 MINUTES OF THE LAST MEETING HELD ON 7 APRIL 2016

The Committee agreed that the minutes of the last meeting held on 7 April 2016 be signed by the Chairman as a true and correct record.

3 STRATEGIC RISK REGISTER - SUSTAINABILITY OF THE COUNCIL

The Committee considered a progress report in relation to the individual risks identified on the Strategic Risk Register, specifically in relation to risks regarding Sustainability of the Council. The Committee discussed plans to control and mitigate the risks with the strategic risk owners, Mr Jack, Chief Executive, Mr Towers, Director of Governance and Partnerships and Mr Thompson, Director of Resources.

Mr Thompson reported that nationally there was a general risk over the sustainability of local government in recent years due to the impact of funding cuts. He noted that whilst there was a statutory duty for local authorities to deliver a balanced budget and some specified services, there were a number of services that were currently delivered despite there being no statutory obligation. It was therefore explained to Members that there were budgetary pressures on the ability of the Council to continue delivering non-statutory services.

MINUTES OF AUDIT COMMITTEE MEETING - THURSDAY, 26 MAY 2016

Mr Thompson reported that despite the repeated cuts to funding, a consistent level of reserves had been maintained throughout the years of austerity, through prudent financial management. He provided Members with details of plans of how the budget would be managed in future, which included the drafting of a six year Medium Term Financial Strategy that should be in place by September 2016.

Mr Towers provided information to the Committee on the sub risk of 'further devolution of services and increased partnership working'. He explained that as decision-making and funding became more localised through projects such as Better Start and Head Start, as well as the development of the Combined Authority proposal, it was important to ensure appropriate governance structures were in place that enabled a sufficient level of scrutiny.

Mr Towers provided Members with examples of the services currently shared with Fylde Council, which included Human Resources and Civic Support. He also provided the Committee with details of the partnership working arrangements that were in place with the Blackpool Teaching Hospitals Trust and noted the role of the Public Services Board in ensuring that public services were shared where possible, in order to deliver the best value for public money.

Mr Jack provided the Committee with information relating to the sub risk of there being 'insufficient Central Government funding for Care Act reforms in addition to current constraints on cash limited budgets'. Mr Jack reported that the Government had since deferred the introduction of the policy to cap the costs of care.

The Committee was also provided with details of the implications of the implementation of the living wage on the Adult Social Care budget. Mr Jack advised that the Adult Social Care budgets in northern areas had been adversely impacted by the introduction of the living wage, compared to the impact in southern areas. He provided Members with details of the shortfall between the additional funding received through the Adult Social Care precept and the actual cost of implementing the living wage. He noted that rises to the living wage above inflation would be factored into the Medium Term Financial Plan.

Members noted that a control for the risk was 'to challenge government assumptions and support lobbying for resource' and raised questions relating to the form of lobbying for resources that was employed. Mr Jack advised that it would depend upon for which service the lobbying was on behalf of and advised Members that the Leader of the Council had a role on the Local Government Association, which had a potential to make a big impact in relation to lobbying government. Mr Jack noted the requirement to work alongside other public sector partners, for instance those in the Health sector, in order for lobbying on behalf of the local area to have a greater impact. Mr Jack also advised that regular meetings were held with both of the MPs representing Blackpool in order to lobby the Government on a number of issues.

Members raised questions relating to budget overspends and Mr Thompson advised that in areas such as Children and Adult services, budgets were subject to volatile levels of demand, with the result that there was a greater potential for there being overspends within the budgets for those services.

MINUTES OF AUDIT COMMITTEE MEETING - THURSDAY, 26 MAY 2016

Members discussed the impact upon services from cuts to local authority funding and Mr Jack advised that savings would become harder to find in future and there would be a requirement to consider which services were the most essential for residents.

Background papers: None.

4 STRATEGIC RISK REGISTER - INEFFECTIVE GOVERNANCE

The Committee considered a progress report in relation to the individual risks identified on the Strategic Risk Register, specifically in relation to risks regarding Ineffective Governance. The Committee discussed plans to control and mitigate the risks with the strategic risk owners, Mr Jack, Chief Executive, Mr Towers, Director of Governance and Partnerships and Mr Thompson, Director of Resources.

Mr Towers provided the Committee with an overview of the sub risk of 'non-compliance with statutory requirements and internal procedures' and the controls that were undertaken to mitigate the risk. He provided details of the work undertaken to raise awareness of the standards of governance required and of the consequences of failure to meet governance standards. He reported to the Committee that an Executive Decisions Toolkit had been developed to ensure managers across the Council were aware of the requirements of governance and decision-making arrangements.

Mr Jack advised Members of some of the control mechanisms in place to mitigate against the quality of services being compromised or Health and Safety being compromised as a result of non-compliance with statutory requirements and internal procedures. He noted that the control mechanisms were appropriately varied and that, as a developing control he would be ensuring that there was a consistent use of Human Resources policies across the Council.

Upon questioning from Members, Ms Greenhalgh explained that the Risk Management Framework set out the requirements for risk registers and the Risk Management Toolkit provided practical advice for managers on how to prepare and use a risk register.

Members also raised questions in relation to the sub risk of an 'increased risk of fraud' and Mr Thompson advised that the increased risk was due to a combination of factors, which included less resource to tackle fraud, as well as other factors prevalent in the current economic climate that made people more likely to attempt to commit fraud.

Background papers: None.

5 RISK SERVICES QUARTER FOUR REPORT - 2015/2016

Ms Greenhalgh, Chief Internal Auditor, presented the Committee with an overview of the Risk Services Report for the fourth quarter of 2015-2016.

MINUTES OF AUDIT COMMITTEE MEETING - THURSDAY, 26 MAY 2016

Ms Greenhalgh provided the Committee with a summary of the key points contained within the report and advised Members that a major incident exercise had been undertaken on 19 January 2016, which had involved a wide range of services. It was reported that the outcome of the exercise had been collated and would help with future learning, especially in relation to Property Management and the development of the Major Emergency Plan.

Ms Greenhalgh reported on the Key Performance Indicators for the service. It was noted that the percentage of professional and technical qualifications held was lower than the target and, upon questioning from Members, Ms Greenhalgh explained that the reason was due to two members of staff with professional qualifications having left the Service. She advised that as a result, junior members of the team were being afforded more opportunities and training.

Members also raised questions relating to the number of trained Emergency Response Group Volunteers and it was reported that plans to increase resilience through employing joint arrangements with Lancashire County Council and Blackburn with Darwen Council, were being investigated. Members were also advised that the possibility of providing incentives for volunteers was also being explored. Mr Jack noted that the volunteers were only required for emergencies occurring outside of office hours and that there would be appropriate numbers of staff to be able to deal with emergencies during office hours.

Members noted that the percentage of risk registers revised and up to date at the end of the quarter was slightly below target and were assured that the indicator was expected to be on target by the end of the Risk Services Quarter One Report 2016/2017.

Members also raised questions in relation to the Corporate Fraud Statistics and were advised that the National Fraud Initiative was a national exercise on data matching. Ms Greenhalgh explained that of the 2,752 referrals that Blackpool had received, 553 had resulted in an investigation of some form. Ms Greenhalgh advised that a risk assessment was completed on every referral received, upon which any further investigation depended. She noted that the Corporate Fraud Team would record if no further action was taken on a referral. The Committee requested that an additional column be inserted into the table of Corporate Fraud Statistics, indicating the number of referrals received, but that no further action had been taken.

Ms Greenhalgh provided the Committee with an overview of the Internal Audit reports issued during Quarter Four, with particular reference to the inadequate statements that had been issued.

The Committee considered the Internal Audit report of the Coastal Communities Fund, for which the controls in place had been assessed as being inadequate due to the lack of a robust income stream that left the project at risk of being unsustainable. It was also noted that there were concerns that the project did not follow a formal project management methodology and key documents, such as project plans and actions plans were not in place. Members noted that it was a three year project with an aim to become self-sufficient in the future, but raised concerns that there was still not a project plan in place after the first year.

MINUTES OF AUDIT COMMITTEE MEETING - THURSDAY, 26 MAY 2016

The Committee discussed plans for income generation for the project and requested that the relevant officer be invited to the next meeting of the Committee to provide an explanation for controls being inadequate and to provide a progress report detailing how the concerns of the audit had been mitigated.

The Committee also considered insurance claims data and Ms Greenhalgh advised that there had been a reduction in the number of tripping claims. It was considered that the reduction in claims was due to a number of factors, which included the impact of Project 30, although at a slower rate than had initially been anticipated, and the Jackson reforms, which had arisen following a review of civil litigation costs. Ms Greenhalgh reported that it was expected that the Highways Road Asset Management Strategy would continue to have an impact in reducing claims further. Members questioned whether Project 30 would deliver the savings that had initially been targeted and were advised that initial targets had been aspirational and there remained a gap between the savings currently achieved and the savings initially forecast.

The Committee agreed:

- 1) To note the report.
- 2) To request that an additional column be inserted into the table of Corporate Fraud Statistics, indicating the number of referrals received but that no further action had been taken.
- 3) To request that the Director of Place be invited to attend the next meeting of the Committee in order to provide an explanation for controls being inadequate in relation to the Coastal Communities Fund internal audit review and to provide a progress report detailing how the concerns of the audit had been mitigated.

Background papers: None.

6 ANNUAL INTERNAL AUDIT OPINION AND QUALITY IMPROVEMENT PROGRAMME

Ms Greenhalgh presented a report to the Committee, which provided Members with details of the Chief Internal Auditor's Annual Opinion on the Council's control environment and details of the Quality Improvement Programme, which the audit team was working towards in line with the Public Sector Internal Audit Standards.

Ms Greenhalgh summarised the key points from the report to Members, advising that she was satisfied that sufficient assurance work had been undertaken in 2015/2016 to allow the provision of a reasonable conclusion on the adequacy and effectiveness of the Council's internal control environment and that her opinion was that the overall control environment of the Council was adequate.

The Committee was provided with details of the planned internal audit reviews that had not been undertaken and the reason for their deferment. The planned reviews had included Housing Benefit Risk Based Verification, which had been deferred until early 2017/2018 for the scheme to be embedded; Public Health Commissioning, which had been deferred until

MINUTES OF AUDIT COMMITTEE MEETING - THURSDAY, 26 MAY 2016

2017/2018 due to potential changes to the model used to provide commissioning services; Governance Arrangements of Boards and Panels, which had been deferred until 2016/2017 to provide assurance that the new arrangements were working effectively; and Identification of Carers, Care and Support, which had been a requirement of the Care Act, however given the delays in the implementation there would be little value in undertaking the review in 2015/2016.

Ms Greenhalgh reported to Members that she was of the opinion that in all material respects the Internal Audit Team conformed to the definition of internal audit, the Code of Ethics and the Public Sector Internal Audit Standards.

The Committee was also presented with the Quality Assurance Improvement Programme Action Plan.

The Committee agreed to note the findings from the Annual Internal Audit Opinion and Quality Improvement Programme.

Background papers: None.

7 AUDIT COMMITTEE TRAINING PROGRAMME 2016/17

The Committee considered the proposed modular training programme for Audit Committee Members.

Members requested that the training on the 'Role of the Audit Committee' was open to all Councillors.

The Committee agreed:

- 1) To approve the Audit Committee training programme.
- 2) To request that the 'Role of the Audit Committee' training was open to all Councillors.

Background papers: None

8 ANNUAL AUDIT FEE 2016/2017

The Committee considered the external auditor's Annual Audit Fee Letter 2016/2017.

Mr Leviston, Manager, KPMG, summarised the annual audit fee letter, which detailed the audit work and fee proposed for the 2016/2017 financial year. He explained that the proposals were based upon the risk-based approach to audit planning as set out in the Code of Audit Practice and Public Sector Audit Appointment's published work programme and fee scales.

The Committee agreed to note the external auditor's Annual Audit Fee Letter 2016/2017.

MINUTES OF AUDIT COMMITTEE MEETING - THURSDAY, 26 MAY 2016

Background papers: None

9 DATE OF NEXT MEETING

The Committee noted the time and date of the next meeting as 6pm on Thursday 30 June 2016 at Town Hall, Blackpool.

Chairman

(The meeting ended at 7.49 pm)

Any queries regarding these minutes, please contact:
Chris Kelly, Senior Democratic Governance Adviser
Tel: 01253 477164
E-mail: chris.kelly@blackpool.gov.uk

This page is intentionally left blank

Report to:	AUDIT COMMITTEE
Relevant Officer:	Alan Cavill, Director of Place
Date of Meeting	30 June 2016

LIGHTPOOL PROJECT – INTERNAL AUDIT

1.0 Purpose of the report:

1.1 To update the Audit Committee on actions taken to address the recommendations of the Internal Audit review on the LightPool project dated 11 February 2016.

2.0 Recommendation(s):

2.1 The Audit Committee is asked to consider the updates on the actions taken.

3.0 Reasons for recommendation(s):

3.1 The update is presented following a request from the Audit Committee at its last meeting on 26 May 2016.

3.2a Is the recommendation contrary to a plan or strategy adopted or approved by the Council? No

3.2b Is the recommendation in accordance with the Council's approved budget? Yes

3.3 Other alternative options to be considered:

None

4.0 Council Priority:

4.1 The relevant Council Priority is "The economy: Maximising growth and opportunity across Blackpool"

5.0 Background Information

5.1 At its meeting of 26 May 2016, the Audit Committee agreed to request that the Director of Place be invited to attend the next meeting of the Committee in order to provide an explanation for controls being inadequate in relation to the LightPool internal audit review and to provide a progress report detailing how the concerns of the audit had been mitigated.

5.2 On 11 February 2016, Internal Audit issued its report on the review of the LightPool project, which had been established to:

- Review the LightPool project business plan and its alignment with the details in the bid document.
- Assess whether the LightPool business plan is robust, setting out aims and measures that will help to facilitate the successful completion of the Illuminations development and enable success in achieving sustainability and wider economic benefits into the long term future.
- Assess whether anticipated outcomes are beginning to be achieved in the first season for LightPool and whether monitoring procedures implemented to date are robust.

5.3 The detailed findings and recommendations of the Internal Audit are included in attached report (Appendix 3a). The Director of Place will be in attendance at the meeting to answer questions from the Committee in relation to the report and update Members on the progress of mitigating the concerns raised in the report.

Does the information submitted include any exempt information?

No

List of Appendices:

Appendix 3a – Internal Audit Report - Review of the LightPool Project.

6.0 Legal considerations:

6.1 None

7.0 Human Resources considerations:

7.1 None

8.0 Equalities considerations:

8.1 None

9.0 Financial considerations:

9.1 Contained within the report (Appendix 3a).

10.0 Risk management considerations:

10.1 Contained within the report (Appendix 3a).

11.0 Ethical considerations:

11.1 None

12.0 Internal/ External Consultation undertaken:

12.1 None

13.0 Background papers:

13.1 None

This page is intentionally left blank

Internal Audit Report

Review of the LightPool Project



Audit Team: Gary Smith
Lisa Hughes
Date: 11th February 2016

1. Scope

1.1 The scope of our audit was to:

- Review the LightPool project business plan and its alignment with the details in the bid document.
- Assess whether the LightPool business plan is robust, setting out aims and measures that will help to facilitate the successful completion of the Illuminations development and enable success in achieving sustainability and wider economic benefits into the long term future.
- Assess whether anticipated outcomes are beginning to be achieved in the first season for LightPool and whether monitoring procedures implemented to date are robust.

2. Executive Summary

2.1 Changes to proposed income streams as stated within the Business Plan have resulted in the project not currently having a robust means of income generation.. The Council has committed to providing a contribution of £296,565 which was based on raising this amount through income streams. As the current methods cannot be relied upon the Council is at risk of having to take these funds from already reduced budgets in order to address the shortfall. Financial forecasting for 2016/17 is still in progress and therefore we are unable to provide assurance at this stage about the robustness of these plans.

2.2 The project is not being delivered in accordance with any formal project management methodology and consequently there is no formal process in place for monitoring progress and implementation of key tasks. A project risk register has been devised but is also not monitored at the board meetings.

2.3 The creation of a LightPool Customer Relations Manager (CRM) database to be used for recording visitor data was planned at the outset of the project but has not yet been implemented. There are currently no plans to create this or introduce an alternative system which could impact on the effectiveness of future data evaluations.

2.4 The service is working closely with the Corporate Development Manager to ensure that outcomes and impacts can be suitably measured. The results from visitor surveys are yet to be evaluated although the Corporate Development Manager responsible for monitoring and evaluation explained that a full report detailing the outcomes for the first season is due to be presented at the February Board meeting.

2.5 The detailed findings and recommendations are included in sections four and five of this report.

2.6 We would like to thank Richard Ryan, Rob Latham, Scott Butterfield, Claire Courtenay and Kirsten Whyatt for their assistance and courtesy throughout the review.

3. Overall Opinion and Assurance Statement

- 3.1 We consider that the controls in place are currently inadequate due to the lack of a robust income stream which leaves the project at risk of incompleteness and being unsustainable. We are also concerned that the project is not following a formal project management methodology and key documents such as project plans and action plans are not in place. Results for anticipated outcomes are not yet available although methods proposed for obtaining these are in development. It is recognised however that the project is still in its first year and implementation of recommendations within this report should help to address these issues.

4. Issues Arising

4.1 Background.

4.1.1 An application was made to the Department for Communities and Local Government (DCLG) for a grant from the Coastal Communities Fund (CCF) in October 2014 for the purpose of creating the LightPool project which is a transformation of the Blackpool Illuminations. The project aims to introduce new elements to the existing attraction which provide greater levels of interaction for visitors.

4.1.2 The Illuminations attract 3 to 4 million visitors to Blackpool each year. The attraction is free to visitors, although there is a suggested donation, and highly dependent on Council funding. The experience is very much a passive one, with the majority of visitors entering the event at one end of the promenade, driving through to the other and then leaving having had little other interaction with the town. A key focus of LightPool is to encourage visitors to leave their vehicles and engage with new elements of the attraction and contribute to the local economy. It is hoped that the new content will provide a greater experience which visitors will be prepared to pay for, or otherwise contribute to the local economy, and in doing so make the Illuminations more financially sustainable.

4.2 LightPool Grant Application alignment to the Business Plan

4.2.1 The grant bid application was prepared by the Project Development and Funding Manager within the Partnerships and Business Development Team. A LightPool Business Plan was also created and this document was submitted as part of the bid application as this was a CCF requirement due to the amount of funding requested.

4.2.2 The Business Plan is a detailed fifty page document also compiled by the Project Development and Funding Manager who has extensive experience in preparing funding bid applications. The Business Plan supports the bid application providing further detail to the information supplied on the application.

4.2.3 Confirmation of a grant award of £1,998,045 has been received from DCLG for the project which comprises a £700,000 capital grant and a £1,298,045 revenue grant. The full capital grant and £740,162 of the revenue grant have been received for the financial year 2015/16 and the remaining revenue grant is due to be received at the beginning of the 2016/17 financial year.

4.2.4 The grant determination letters explain that the grant is paid under Section 31 of the Local Government Act 2003. A condition of such grants is that the recipient authority's Chief Executive and Chief Internal Auditor must complete a declaration for any capital element confirming that funding has been used solely for capital purposes. This declaration should be received by DCLG by 30th January 2017 and failure to comply could result in repayment of all or part of the grant. It is therefore essential that the service ensures that Internal Audit and the Chief Executive are

informed of their requirements to ensure that resources are available to complete the declaration at the appropriate time and that adequate records are made available for this purpose (Recommendation 1).

4.2.5 Furthermore, the CCF's standard terms and conditions of grant state that the progress of the project should be monitored and monitoring forms as issued by CCF should be completed. The terms also state that the grant should be used exclusively for the project and that any unused monies must be repaid, however there is no reference to clawback of funding if outcomes are not achieved. There is no stated deadline for this monitoring although the service has already started the work in anticipation of its completion in the next couple of months. The return requires the service to provide details of the outcomes achieved within the year and where possible details of case studies of those benefiting from the project. Details of outcomes will be obtained from the planned monitoring and evaluation which is further described at section 4.4 of this report.

4.2.6 Match funding by the Council was not a stipulation of the grant award, however the Council committed to contributing £296,565 to the project as part of the bid application which the Director of Place has agreed will need to be met from his overall directorate budget if this is not met by income generated from the project as is planned. LeftCoast, a local arts and creative activity programme funded by the Arts Council, have also confirmed in writing that they will contribute a total of £120,000 to the project.

4.3 LightPool Business Plan and Project Management

4.3.1 The Business Plan sets out the aims of the LightPool project and lists the practical measures that will be put in place to achieve these aims. The project's aim is to deliver a radical transformation of the Blackpool Illuminations, create a new visitor experience and encourage a major boost to the local economy. The project also aims to create 11.6 (full time equivalent) direct jobs, 532 indirect jobs over a period of 5 years, 2.65million new visitors over a period of 5 years and to safeguard 15 existing direct jobs. It is intended to act as a catalyst towards providing a more sustainable business model for the illuminations which currently relies on Council funding.

4.3.2 The Business Plan states that the headline attraction will be the creation of a new digitally mapped projection show onto the front of Blackpool Tower accompanied by audio via in-ear FM receivers which visitors will be provided with in a LightPool goody bag containing a map, light based toy and discount vouchers for retailers and attractions. The Business Plan states that these will be charged for as a means of generating income for the sustainability of the project. However, we have noted that the financial forecast which was submitted as part of the business plan relied on the projected income from the sale of the goody bags, however these sales did not go ahead in year one of the project. Further proposed new elements of the project are described within the Business Plan and include programmable digital LED festooning which will stretch along the Promenade between North and Central Piers which may be programmed to interact with the projection show. The festooning will also extend into key streets in the town centre and will be able to fully interact with the promenade display. It is intended that those watching the projection show will be encouraged to follow the festooning into the town centre, creating additional footfall and a boost to the local economy.

4.3.3 One key area that the festooning will lead to is the existing Brilliance light installation on Birley Street. The Business Plan explains that this area will be transformed into an events space for outdoor performances throughout the year which could incorporate the daytime cafes also located on Birley Street into night time venues and consequently bring more economic benefit to the town. As Birley Street is a major departure route for visitors leaving other large scale events such as the fireworks championships Brilliance will provide another attraction to keep visitors in the town.

4.3.4 Both the projection show and the digital LED festooning were in place and ready for the 2015 Illuminations period with the first of the projection shows launched in September 2015. A programme of events also took place at the outdoor Brilliance feature.

4.3.5 The Business Plan also describes a further attraction to be based in the Grundy Art Gallery during the illuminations period which features an indoor light installation and offer an additional attraction for visitors during the daytime. These shows took place during the Illuminations period and the curator of the gallery reported at the September 2015 Board meeting that they had received a good response and visitor numbers had doubled compared to the same period last year.

4.3.6 The current financial forecast provided by the Project Accountant shows that there will be a net underspend of £25,000 at the end of 2015/16 which will be carried forward to next year. Although less income was received, expenditure was lower than expected in the first year. The income target for 2016/17 currently stands at £241,000, however the accountant has explained that this forecast needs updating and they are due to review this with the Project Manager. The current forecast relies on the sales of goody bags for the generation of income and as this income stream is no longer considered feasible we recommend that the income strategy is revised to reflect the decisions made during the first year of the project and financial forecasts are updated accordingly (Recommendation 2).

4.3.7 The Project Manager explained that plans for income generation for the LightPool project now rely heavily on sponsorship deals. The delay in recruiting the Business Development and Fundraising Manager has hindered income generation but now that the post has been filled an event has been arranged in February 2016 for pitching to local and national businesses for sponsorship. Laurence Llewelyn-Bowen, who has previously designed some of the illuminations, has agreed to attend as a guest speaker. The Illuminations service currently receives some income from sponsorship deals and in 2015/16 the service generated approximately £140,000. There is a remaining income target for the year of approximately £110,000 for the Illuminations service as a whole which is hoped to be found through further sponsorships in future years but is a known budget pressure for 2015/16.

4.3.8 A small amount of income, approximately £6,690, was received from the photo projection booth. This was an idea that developed during implementation that was not in the original plan and allows visitors to have their image projected onto the front of Blackpool Tower. A charge of £2 per person was made for this and it is hoped to further develop the idea during 2016 to include an emailed photograph of the image to the visitor for an additional fee.

4.3.9 Accountability for the project is detailed in the Business Plan with overall responsibility for the project resting with the Director of Place. The Head of Illuminations has been assigned the role of Project Manager and is responsible for overseeing the day to day running of the project. A Project Board has also been set up which also includes the Head of Visitor Economy, Head of Arts, Head of Leisure and Catering Services and representatives from Accountancy, the Winter Gardens, Merlin and LeftCoast. Board meeting minutes were obtained and showed that meetings are held monthly and well attended. A set format is followed which includes a review of key tasks and an action column detailing the responsible officer's initials.

4.3.10 A Project Risk Register has been produced and was included as part of the Business Plan. This was devised following a risk workshop facilitated by the Council's Chief Internal Auditor. Our review of Board meeting minutes however, showed that the register is not reviewed as an independent item at meetings to ensure outstanding risks are addressed. We therefore recommend that the risk register is reviewed at future Board meetings and updated as appropriate (Recommendation 3).

4.3.11 The project is not being delivered in accordance with a formal project management methodology and there is no formal process for monitoring progress. An initial project timetable was submitted as part of the Business Plan but this has not been updated. The Project Manager explained that he is in the process of devising an action plan that will be monitored going forward. Application of a project management methodology would drive the production of relevant project management documentation such as a project plan and ensure the regular monitoring and delivery

of key tasks. We therefore recommend that a suitable project management methodology is followed (Recommendation 4).

4.3.12 One of the project aims is to create the following posts: Creative Director, Business Development and Fundraising Manager, Administrator, 16 Ambassador roles, two Technical Apprentices and a Technical Assistant. Some of these roles are seasonal or part-time equating to 11.6 full-time equivalents overall. The Business Plan explains that the Creative Director will determine illuminations content and the programming of all events and the Business Development and Fundraising Manager will support fundraising activity including sponsorship. The Ambassadors will act as stewards and provide a point of contact for visitors and will receive WorldHost customer care training. They will also be complemented by a pool of volunteer Ambassadors. Technical staff will learn how to operate the projection equipment and as a result operate future shows.

4.3.13 All posts have now been recruited to, although the Creative Director and Business Development and Fundraising Manager roles have only recently been filled. The volunteer Ambassadors were not recruited during the first year but it is intended to have them in place for 2016/17 and the Blackpool, Wyre and Fylde Volunteer Centre has agreed to help to provide these staff. The Creative Director post, initially advertised as a full time post has now been filled with two part time staff. The apprentice roles are permanent whereas all other roles are temporary for the duration of the project. The Business Plan states however that the Council is committed to continue to support these new roles through its planned new income sources.

4.3.14 The Business Plan includes a detailed Marketing and Communications Strategy to be led by Visit Blackpool with a proposed budget of £361,500 for the first two years. However, changes to the original plan have since been made. The initial strategy was produced by Amion Consulting, specialist advisers on economic growth, who recommended this budget figure. On submission of the funding bid, DCLG explained that in order to gain project approval the marketing budget would need to be reduced. As a result, a revised two year budget of £99,000 was assigned and a new marketing plan has been developed and is being led by Visit Blackpool's Marketing Manager. At the time of our review, the accountant had received limited details of marketing spend from the marketing manager although total spend has since been confirmed as £51,300. In order to ensure that financial forecasts reflect an accurate picture of project costs, we recommend that details of future marketing costs are provided on a regular basis (Recommendation 5).

4.3.15 A Monitoring and Evaluation Framework is also included in the Business Plan which sets out how outputs and indicators as stated in the project bid application will be measured. Examples of measures include visitor numbers, specific visitors to LightPool and jobs created. This information is required to complete the annual monitoring return required by CCF.

4.3.16 The framework focuses on the use of visitor surveys, an economic impact report and use of a LightPool CRM database for recording visitor data. Data from the Council's Omnibus survey and a LightPool Visitors survey has so far been collated. The Omnibus survey is used by the Council to collect visitor data three times a year from a random sample of 4,000 households across the country. Questions relating to LightPool were included in the September – December survey and the results from this are due to be received in January 2016. The LightPool visitors survey was a street survey of 997 visitors in the town centre during the LightPool period and was co-ordinated by Infusion Research.

4.3.17 The CRM database has not been set up and the Project Manager explained that a decision is yet to be made as to whether to go ahead with this. We recommend that a decision as to whether this is still required should be made as soon as possible and if not, to explore whether another method for recording visitor data is required (Recommendation 6).

4.4 Business Plan Monitoring and Evaluation

4.4.1 The results from both the Omnibus and LightPool Visitors surveys are yet to be evaluated although the Corporate Development Manager responsible for monitoring and evaluation explained that a full report detailing the outcomes for the first season is due to be presented at the February Board meeting.

4.4.2 In addition to these surveys it is planned to commission an update of the Blackpool Illuminations Economic Impact report which will measure key indicators including direct and indirect tourism impacts, employment impacts, and the impact of spending on goods and services. The Corporate Development Manager explained this will be implemented at the end of the project in approximately February 2017. As information from this survey will be used to complete the annual CCF return there is a risk that commissioning this report in February 2017 may not provide enough time for collation and analysis of results prior to the year-end deadline and it is therefore recommended that the timing of this report is reviewed (Recommendation 7).

4.4.3 Local business surveys are also due to be commissioned. These will measure growth, size, turnover and perceptions of the impact of LightPool. The Corporate Development Manager explained these surveys will most likely take the form of face to face visits and are scheduled for November 2016.

5. Agreed Action Plan

Page 20

	<i>Recommendation</i>	<i>Priority</i>	<i>Agreed Action</i>	<i>Responsible officer</i>	<i>Target Date</i>
R1	Internal Audit and the Chief Executive should be informed of their requirements in relation to completing the capital grant declaration.	3	Agreed. The Project Manager will advise accordingly.	Head of Illuminations	31/03/16
R2	The income strategy should be reviewed and financial forecasts revised to take account of this.	1	Agreed.	Head of Visitor Economy	31/03/16
R3	The project risk register should be included for discussion at Board meetings to ensure that appropriate mitigations are being taken to reduce the risks.	2	Agreed. This will be included at Project Board meetings.	Director of Place	29/02/16
R4	An appropriate project management methodology should be followed and key documents, such as a project plan, should be monitored by the Board to ensure that they are delivered.	1	Agreed. A Project Plan will be devised and monitored by the Project Board.	Head of Illuminations	31/03/16
R5	Expenditure on marketing activity should be provided to accountancy on a regular basis to enable this to be built into project costs.	2	Agreed.	Head of Visitor Economy	29/02/16 and ongoing.

Key to Priorities

Priority 1	A recommendation we view as essential to address a high risk
Priority 2	A recommendation we view as necessary to address a moderate risk.
Priority 3	A recommendation that, in our opinion, represents best practice or addresses a low level of risk.

**Blackpool Council: Internal Audit
Assuring Quality Services for Blackpool**

<i>Recommendation</i>		<i>Priority</i>	<i>Agreed Action</i>	<i>Responsible officer</i>	<i>Target Date</i>
R6	A decision should be made as to whether the LightPool CRM database is still required.	2	Agreed. The matter will be raised at the next Board meeting.	Head of Visitor Economy	31/03/16
R7	The timing of the commissioning of the Blackpool Illuminations Economic Impact report should be reviewed to ensure results will be available in time to complete year end monitoring forms.	3	Agreed. The Project Manager will discuss with the Corporate Development Manager.	Head of Illuminations	29/02/16

Key to Priorities

Priority 1	A recommendation we view as essential to address a high risk
Priority 2	A recommendation we view as necessary to address a moderate risk.
Priority 3	A recommendation that, in our opinion, represents best practice or addresses a low level of risk.

This page is intentionally left blank

Report to:	AUDIT COMMITTEE
Relevant Officers:	Neil Jack, Chief Executive Steve Thompson, Director of Resources Delyth Curtis, Director of People Arif Rajpura, Director of Public Health
Date of Meeting	30 June 2016

STRATEGIC RISK REGISTER - INABILITY TO RESPOND TO A MAJOR INCIDENT

1.0 Purpose of the report:

1.1 The Committee to consider a progress report on individual risks identified in the Council's Strategic Risk Register.

2.0 Recommendation(s):

2.1 To question the Chief Executive, Director of Resources, Director of People and Director of Public Health on identified risks on the Strategic Risk Register in relation to sustainability of the Council.

3.0 Reasons for recommendation(s):

3.1 To enable the Committee to consider an update and progress report in relation to an individual risk identified on the Strategic Risk Register.

3.2a Is the recommendation contrary to a plan or strategy adopted or approved by the Council? No

3.2b Is the recommendation in accordance with the Council's approved budget? Yes

3.3 Other alternative options to be considered:

To not receive an update report, however this would prevent the Committee from monitoring and asking relevant questions of the Strategic Risk Owners in relation to significant risks identified on the Strategic Risk Register.

4.0 Council Priority:

4.1 The relevant Council Priorities are

“The economy: Maximising growth and opportunity across Blackpool”
“Communities: Creating stronger communities and increasing resilience”

5.0 Background Information

5.1 At its meeting in September 2015, the Audit Committee agreed to continue to invite Strategic Risk Owners to attend future meetings to provide updates and progress reports in relation to the individual risks identified on the Strategic Risk Register.

5.2 Does the information submitted include any exempt information? No

5.3 List of Appendices:

Appendix 4(a) - Excerpt from Strategic Risk Register

6.0 Legal considerations:

6.1 None

7.0 Human Resources considerations:

7.1 None

8.0 Equalities considerations:

8.1 None

9.0 Financial considerations:

9.1 None

10.0 Risk management considerations:

10.1 None

11.0 Internal/ External Consultation undertaken:

11.1 None

12.0 Background papers:

12.1 None

Risk	Sub No	Sub Risk	Impact / Consequences	Opportunity	Gross Risk Score			Controls and Mitigation	Net Risk Score			New Developing Controls	Risk Manager	CLT Risk Owner	Target Date	Corporate Priority
					I	L	GS		I	L	NS					
Inability to Respond to a Major Incident.	9a	Reduced capacity across the Council to respond to an emergency.	May not be able to provide all the resources required as a Category One Responder.	Corporate approach to responding to incidents.	5	4	20	Major Emergency Plan in place outlining roles and responsibilities.	4	4	16	Develop robust arrangements for out of hours cover for critical services.	Deputy Chief Executive	Chief Executive	Ongoing	Safeguarding and protecting
			Potential public enquiry if the incident was not dealt with effectively.									Establish a control centre at Bickerstaffe House for dealing with a major incident.	Chief Internal Auditor / Head of Property and Asset Management	Director of Resources		
			Arrangements need to be agreed and implemented for public health incidents such as Pandemic or Infectious Outbreaks. A decision needs to be taken as to whether this is a separate plan or whether a section is included in all business continuity plans.									Public Health Practitioner / Chief Internal Auditor	Director of Public Health			

9b	Disruption to community, services and businesses.	Loss of community cohesion and potential reputational damage.		5	4	20	Planning for potential incidents through the Lancashire Resilience Forum.	4	4	16	Undertake an exercise on dealing with a major incident in Blackpool and establish what additional controls need to be put in place based on lessons learned.	Chief Internal Auditor	Director of Resources	Ongoing	Safeguarding and protecting
							Community risk register in place.				Roll-out a training programme for those involved in providing a tactical response in a major incident.	Chief Internal Auditor			
9c	Injury / death to members of the public or staff.	Trauma faced by families and work colleagues.		5	4	20	Emergency response group in place to provide humanitarian support in a major emergency.	4	4	16	Increase the number of volunteers on the emergency response group and attend the Lancashire Resilience Forum Humanitarian Assistance Group.	Deputy Director - Adult Services	Director of People	Ongoing	Safeguarding and protecting

Report to:	AUDIT COMMITTEE
Relevant Officers:	Tracy Greenhalgh, Chief Internal Auditor Steve Thompson, Director of Resources Mark Towers, Director of Governance and Partnerships
Date of Meeting	30 June 2016

ANNUAL GOVERNANCE STATEMENT 2015/2016

1.0 Purpose of the report:

1.1 To consider the Annual Governance Statement for 2015/2016.

2.0 Recommendation(s):

2.1 The Audit Committee is asked to approve the Annual Governance Statement for 2015/2016 and consider undertaking a mid-year review of progress against the actions outlined in the Annual Governance Statement.

3.0 Reasons for recommendation(s):

3.1 The Accounts and Audit Regulations (2015) require the Council to conduct a review on the effectiveness of its system of internal control and publish an Annual Governance Statement with the Statement of Accounts.

3.2a Is the recommendation contrary to a plan or strategy adopted or approved by the Council? No

3.2b Is the recommendation in accordance with the Council's approved budget? Yes

3.3 Other alternative options to be considered:

None.

4.0 Council Priority:

4.1 The relevant Council Priorities are

“The economy: Maximising growth and opportunity across Blackpool”

“Communities: Creating stronger communities and increasing resilience”

5.0 Background Information

5.1 Blackpool Council is responsible for ensuring that its business is conducted in accordance with the law and proper standards. It needs to ensure that public money is safeguarded, properly accounted for and used economically, efficiently and effectively.

The CIPFA Delivering Good Governance publication (2016) defines the various principles of good governance in the public sector and how they relate to each other and are defined as:

- Behaving with integrity, demonstrating strong commitment to ethical values and respecting the rule of law.
- Ensuring openness and comprehensive stakeholder engagement.
- Defining outcomes in terms of sustainable economic, social and environmental benefits.
- Determining the interventions necessary to optimise the achievement of the intended outcomes.
- Developing the Council's capacity, including its leadership and the individuals within it.
- Managing risks and performance through robust internal control and strong public financial management.
- Implementing good practices in transparency, reporting and audit, to deliver effective accountability.

The governance framework at Blackpool Council comprises the systems and processes, culture and values which the Council has adopted in order to deliver on the above principles. The system of internal control is a significant part of the framework and is designed to manage risk to a reasonable level. It cannot eliminate all risk of failure to achieve policies and objectives and can therefore only provide reasonable and not absolute assurance of effectiveness.

The governance framework incorporated into this report has been in place at Blackpool Council for the year ended 31 March 2016 and up to the date of the approval for the statement of accounts for that year.

Does the information submitted include any exempt information?

No

List of Appendices:

Appendix 5a – Annual Governance Statement 2015/2016

6.0 Legal considerations:

6.1 The Accounts and Audit Regulations (2015) require the Council to conduct a review, at least once a year, on the effectiveness of its system of internal control and include an Annual Governance Statement reporting on the review with the Statement of Accounts.

7.0 Human Resources considerations:

7.1 None.

8.0 Equalities considerations:

8.1 None.

9.0 Financial considerations:

9.1 Each of the actions identified in the Annual Governance Statement will be delivered within the constraints of the agreed budget for 2016/2017.

10.0 Risk management considerations:

10.1 Risk management and the control environment have been considered throughout the preparation of the Annual Governance Statement 2016/2017.

11.0 Ethical considerations:

11.1 None.

12.0 Internal/ External Consultation undertaken:

12.1 An Annual Governance Statement Review Group was established in February 2016 and has led on the review of effectiveness and the production of the Annual Governance Statement. This group comprised of the Chief Internal Auditor, Director of Governance and Partnerships, Head of Democratic Governance and Head of Corporate Development, Engagement and Communications.

12.2 A workshop was held on the 15 March 2016 with representation from the Audit Committee, Tourism, Economy and Resources Scrutiny Committee, Standards Committee and Cabinet and facilitated by the Chief Internal Auditor, Head of Democratic Governance and Head of Corporate Development, Engagement and Communications.

12.3 A workshop was held on the 25 April 2016 with key officers involved in governance. This included the Chief Internal Auditor, Director of Governance and Partnerships, Head of Democratic Governance, Head of Organisation and Workforce Development, Head of ICT, Chief Accountant and Corporate Development Manager.

12.4 The Corporate Leadership Team was required to complete a control self-assessment questionnaire providing assurance that their directorates were compliant with a number of key controls.

13.0 Background papers:

13.1 None.

Annual Governance Statement 2015/2016

Blackpool Council



Annual Governance Statement 2015/2016

Acknowledgement of Responsibility

Blackpool Council is responsible for ensuring that its business is conducted in accordance with the law and proper standards. It needs to ensure that public money is safeguarded, properly accounted for and used economically, efficiently and effectively.

The Accounts and Audit Regulations (2015) require the Council to conduct a review, at least once a year, on the effectiveness of its system of internal control and include an Annual Governance Statement reporting on the review with the Statement of Accounts.

The Principles of Good Governance

The CIPFA Delivering Good Governance publication (2016) defines the various principles of good governance in the public sector and how they relate to each other and are defined as:

- Behaving with integrity, demonstrating strong commitment to ethical values and respecting the rule of law.
- Ensuring openness and comprehensive stakeholder engagement.
- Defining outcomes in terms of sustainable economic, social and environmental benefits.
- Determining the interventions necessary to optimise the achievement of the intended outcomes.
- Developing the Council's capacity, including its leadership and the individuals within it.
- Managing risks and performance through robust internal control and strong public financial management.
- Implementing good practices in transparency, reporting and audit, to deliver effective accountability.

The governance framework at Blackpool Council comprises the systems and processes, culture and values which the Council has adopted in order to deliver on the above principles. The system of internal control is a significant part of the framework and is designed to manage risk to a reasonable level. It cannot eliminate all risk of failure to achieve policies and objectives and can therefore only provide reasonable and not absolute assurance of effectiveness.

The governance framework incorporated into this report has been in place at Blackpool Council for the year ended 31st March 2016 and up to the date of the approval for the statement of accounts for that year.

The Governance Framework

The key elements of the structures and processes that comprise Blackpool Council's governance arrangements are summarised below.

Annual Governance Statement 2015/2016

Code of Conduct and Behaviours

Codes of Conduct are in place which define standards of behaviours for elected members and officers. Adherence to these is a key part of good governance. These are further supported by the Council's Whistleblowing Policy, Registers of Interests and Gifts and Hospitality Policies. Processes are in place to deal with non-compliance through the Council's Disciplinary Policy for Officers and the Monitoring Officer and/or Standards Committee for Elected Members.

The Council has developed a set of values which all elected members and officers should adhere to when carrying out their duties and these include being accountable, compassionate, delivering quality services, being trustworthy and fair. Work commenced in the year to develop a Leadership Charter which will set out the principles of behaviours for managers and this is being produced in consultation with the Senior Leadership Team.

In the year a set of Ethical Principles was developed which has further enhanced the arrangements in place to ensure that the Council behaves in an ethical manner.

The Council strives to deliver equal opportunities to all and equality impact assessments form a part of the decision making process. A dedicated Equalities and Diversity Team is in place at the Council to support managers in discharging their duties.

Commitment to Openness, Communication and Consultation

The Council complies with the Transparency Agenda and provides a wide range of information in the public domain through its website. Key messages are also communicated to residents in the Your Blackpool publication which is delivered to all Blackpool households on a quarterly basis. Social media is used on a regular basis and is proving an effective way to provide the community with important information from the Council. The public are able to attend and speak at Committee meetings and Full Council is broadcast on the Council's website.

The Council consults and engages with a diverse cross-section of the community to help to ensure that their views are considered. Examples of consultation exercises include household surveys and the Council Couch where Council Officers go out into the community to listen to what residents have to say.

Developing, Communicating and Translating the Vision

The Council Plan 2015-2020 sets out the vision for Blackpool to be *'The UK's number one family resort with a thriving economy that supports a happy and healthy community who are proud of this unique town'*. This is supported by the two priorities for the Council which are:

- The Economy: Maximising Growth and Opportunity across Blackpool.
- Communities: Creating Stronger Communities and Increasing Resilience.

The length of the Council Plan has been reduced and the style in which the plan is written reviewed to ensure that the document is accessible and understandable to employees and residents and the plan contents were agreed following a consultation exercise.

A staff conference was held in the year, hosted by the Chief Executive, which formally launched the plan and the Council's priorities to employees.

Annual Governance Statement 2015/2016

Beneath each priority the plan details the key challenges faced by Blackpool and the key projects and schemes which will be implemented to address these issues.

The Council Plan seeks to address the big issues and policy drivers facing local government. The Council priorities feed into directorate business plans and are a key tool for managers to use when developing business plans.

Performance Management

A Policy Framework is in place which sets out the corporate strategies and plans which are in place and the Corporate Development Team have a role in the production, monitoring and management of these key documents.

The Council has reviewed and refined its performance management system and strategic performance is reported to the Corporate Leadership Team and the relevant Scrutiny Committees with local performance indicators being managed through the Business Planning Process.

In order to improve performance the Council participates in peer reviews and benchmarking exercises to learn from others and to ensure that services delivered are value for money.

Staff performance is managed through team meetings, one to ones and the Individual Performance Appraisal process. A Capability Policy is in place to manage the performance of employees who are not delivering to the appropriate standard.

Roles and Responsibilities

Responsibilities and functions are in place for each Council Committee including Licensing, Planning, Standards, Scrutiny and Audit Committee. These are reviewed annually with any changes made at the Council's Annual Meeting to ensure that they continue to be fit for purpose. The Executive has agreed a set of criteria relating to the levels of decision making which provide clarity relating to levels of decision making which provide clarity and consistency for decision makers. This has also been reviewed and refined in the last twelve months.

All Council Officers, including the Corporate Leadership Team, have a job description which sets out their roles and responsibilities. Individual objectives for each officer are then part of the Individual Performance Appraisal process and managers have an additional mandatory set of manager objectives which they must conform with.

The Council's Constitution, including the Scheme of Delegation, sets out the arrangements and protocols which are in place to enable effective communication within the authority and they also identify arrangements for working with partners.

The Council has in place effective arrangements to discharge the Head of Paid Service function and this role is undertaken by the Chief Executive.

The Council has designated a Monitoring Officer and Deputy with appropriate qualifications and experience. The Monitoring Officer has the specific duty to ensure that the Council, its officers and its Elected Members maintain the highest standards in all they do and is responsible to Blackpool Council for ensuring that governance procedures are followed and all applicable statutes and regulations are complied with.

Annual Governance Statement 2015/2016

Decision Making

The Constitution sets out the functions and responsibilities of the Council, the Executive and Committees. Included in this are the delegation arrangements adopted by the Council and the Executive and this is reviewed on a regular basis.

All Executive Decisions contain all relevant policy implications including financial, risk management, human resources, equality analysis, ethical considerations, legal considerations and links to Council priorities. All Executive Decisions are subject to finance and legal approval before they are taken forward for a decision to be made. The Monitoring Officer or a designated representative, receive all decisions before they are processed and therefore are able to check the robustness of data quality prior to a decision being submitted for formal approval.

Cabinet Member and relevant Officer Decisions are published to meet transparency requirements and inform the public.

A framework for undertaking compliance checks to ensure that decision making processes are appropriate has been developed and these reviews are jointly carried out by Internal Audit and Democratic Governance and the findings reported to Audit Committee.

Compliance with relevant Laws, Regulations, Internal Policies and Procedures

A wide range of corporate policies and procedures are in place to ensure compliance with laws and regulations. These cover all key areas including financial management, human resources, procurement, contract management, risk management, business continuity, data protection, health and safety management arrangements and safeguarding arrangements.

Managers are responsible for ensuring that their service adheres to the relevant policies and procedures and Disciplinary and Capability Procedures are in place to deal with non-compliance.

Internal and external audit arrangements are in place to provide a reasonable level of assurance with compliance of the Council's system of internal control and the Health and Safety Team also undertake a programme of audits to ensure that managers maintain their manuals.

Mandatory training is delivered through the I-pool online system to advise staff of legislative requirements covering Induction, Child Sexual Exploitation, Customer Care, Data Protection Awareness, Equality and Diversity Awareness, Fire Safety Awareness, ICT Security, Infection Control, Safeguarding and Protection of Adults, Safeguarding Children and You and Your Workstation. Completion rates are reported to the Corporate Leadership Team so that action can be taken in services where non-completion is evident.

The Council's Monitoring Officer has a role in ensuring that the Council acts within the remit of relevant law and regulations and that a robust democratic process is maintained.

A number of arrangements are in place to deal with potential breaches to compliance and these include a Data Breach Panel, Corporate Complaints Panel, Serious Case Reviews and a Disclosure and Barring Service Panel. These are chaired independently of the service which has breached requirements to ensure that objective decisions can be taken.

Annual Governance Statement 2015/2016

Financial Management

The Council has an appropriately qualified and experienced designated Chief Financial Officer who holds Section 151 responsibilities and a deputy has also been appointed. The Chief Financial Officer has arrangements in place for financial management, financial reporting and value for money which is assessed annually by the Council's external auditors.

Financial Regulations are in place which are supported by a Scheme of Delegation to ensure that managers are aware of the level of expenditure they are able to authorise.

Monthly financial monitoring reports, starting from month 0, are reported to the Corporate Leadership Team, the Executive and Tourism, Economy and Resources Scrutiny Committee.

The Council's financial management arrangements conform to the governance requirements of the CIPFA Statement on the Role of the Chief Financial Officer in Local Government (2016).

The Council facilitates a Public Inspection of the Accounts and publishes details of all payment transactions in line with the requirements of the Transparency Code.

Audit Arrangements

An Audit Committee is in place which is independent of the scrutiny function. As a full committee of the Council it is able to discharge all the core functions of an Audit Committee outlined in the CIPFA Audit Committee: Practical Guidance for Local Authorities (2013), from which the Committee has adopted the model terms of reference. Over the past twelve months that Chair of the Audit Committee has taken steps to raise the profile of the Audit Committee and has presented a report to Full Council on the work of the Committee and has proactively requested Chief Officers to attend Committee to be challenged and held to account where controls issues have been identified.

Modular training is delivered prior to each Audit Committee meeting to ensure that members have the appropriate skills and knowledge to effectively discharge their duties. The Audit Committee undertake periodic self-assessments of their performance to identify strengths and areas for development.

The Council has an internal audit team who prepare an Annual Internal Audit Plan which is approved by the Corporate Leadership Team and Audit Committee. This includes a balance of risk and compliance work. The assurance statement for each audit is reported quarterly to the Audit Committee.

In 2015/16 the Chief Internal Auditor's Annual Audit Opinion was that sufficient assurance work was undertaken to provide a reasonable conclusion on the adequacy and effectiveness of the control environment and that the overall control environment at the Council is adequate.

The Council's internal audit arrangements broadly conform to the governance requirements of the CIPFA Statement on the Role of the Head of Internal Audit (2010) and the Public Sector Internal Audit Standards. An external review of the Council's compliance with the Public Sector Internal Audit Standards is planned for 2016/17.

External audit arrangements are in place and they are invited to attend Audit Committee on a regular basis to present the findings of their work and raise any concerns which they may have. Effective working relationships

Annual Governance Statement 2015/2016

are in place with external audit which help ensure that the Council provides timely support, information and responses to the external auditors and considers audit findings and recommendations.

Risk Management

A Corporate Risk Management Group is in place to coordinate and promote risk management activity in line with the Council's Risk Management Framework 2014-2017. It is supported by directorate and thematic risk management groups. An example of the work completed by these groups would be the review and relaunch of the Driving at Work Arrangements by the Driving at Work Risk Management Group due to the risks associated with driving at work and the number of insurance claims which the Council receives in this area.

All directorates have nominated risk champions to promote best practice in their areas and ensure that service level risk registers are in place and that risk registers are developed for major projects and partnerships where appropriate.

The Strategic Risk Register is reviewed by the Corporate Leadership Team every six-months and considered by the Audit Committee annually. Chief Officers identified in the Strategic Risk Register are required to attend Audit Committee to explain how the risks are being managed and what further mitigating controls may be required.

Risk management should be considered for all decisions made by the Council and these are evidenced in the dedicated section on the decision making template.

A Corporate Business Continuity Plan and Critical Activities List are in place and this is supported by service level business continuity plans. Significant work has been undertaken in 2015/16 to improve the quality of the business continuity plans in place.

Counter Fraud and Anti-Corruption Arrangements

The Council has developed counter fraud and anti-corruption arrangements in line with the CIPFA Code of Practice on Managing the Risk of Fraud and Corruption (2014). An Anti-Fraud and Corruption Statement is in place and this is approved by the Corporate Leadership Team and Audit Committee on an annual basis. Any suspected instance of fraud or corruption is reported to the Chief Internal Auditor so that an appropriate investigation into the matter can be undertaken.

A dedicated Counter Fraud Team is in place which will deal with a range of corporate fraud issues and work has commenced on areas of perceived high risk such as insurance fraud. A fraud risk register is in place and this will be further enhanced to continue to inform the Proactive Anti-Fraud Plan.

The Council has appropriate procedures in place to deal with the risk of money laundering and also to raise awareness of the Bribery Act and ensure that appropriate controls are in place to reduce the risk.

The Council participates in the National Fraud Initiative and progress against this, and outcomes, are reported to Audit Committee on quarterly basis.

A corporate group is in place to review the Council's use of covert surveillance and to ensure compliance with the Regulatory of Powers Act (2000). Where covert surveillance is used by the Council this is reported to Audit Committee each quarter to aid with transparency.

Annual Governance Statement 2015/2016

Scrutiny Arrangements

Two Scrutiny Committees are in place which aligns to the Council's priorities including a Resilient Communities Scrutiny Committee and a Tourism, Economy and Resources Scrutiny Committee. These committees help empower elected members and provide them with the opportunity to challenge and hold decision makers to account. Both Committees meet on a regular basis and the minutes of the meetings and supporting documentation are published.

Learning and Development

The Council has obtained Silver Investors in People status demonstrating its commitment to the provision of training to help develop the workforce. A wide range of training is available corporately which is informed from development needs identified in the Individual Performance Appraisal. The Council is an accredited centre for the Institute of Leadership and Management and there has been a commitment to leadership development throughout the year for senior officer and elected members. The attainment of professional qualifications in relevant disciplines is encouraged and the Council is committed to funding studies where appropriate.

A People Strategy is in place and steps are being taken to better align workforce planning with the business plan process however it is recognised that this is in its infancy. An aspiring leadership programme has been delivered to aid with succession planning and provide a development opportunity for managers wishing to progress in the organisation.

The Council runs an apprentice programme to encourage young people and those who may have struggled to access work previously to engage in employment with the Council. Project Search, the job scheme for young people with learning disabilities also ran for a second year where each of the students learn personal and job skills for a two month period before embarking on work placements to find a suitable job for them.

An induction programme is in place for all elected members. A three year development plan is in place for elected members which helps deliver training to elected members to help them fulfil their role. All elected members have a personal development plan which helps to identify training needs.

Partnerships and Joint Working

The Council is involved in a number of key projects with partner organisations in order to transform the way in which services are delivered. Examples include the Better Start Project and Head Start Project which focus on early intervention in order to build resilience in the community. Boards with representation from partner organisations are also in place for key risks faced by the Council to introduce an element of independence and challenge. Examples including the "Getting to Good Board" which aims to address the way in which children's social care is delivered and the Challenge Board to improve educational attainment.

Arrangements are in place for the provision of Shared Services with Fylde Borough Council in a number of areas, the most significant being the Revenues and Benefits Service. The Council is also working jointly with other Fylde Coast authorities on the development of an enterprise zone to improve the local economy.

The Council has a number of wholly-owned companies and a Good Governance Framework has been developed has been rolled-out across each company in order to strengthen the governance arrangements in place and

Annual Governance Statement 2015/2016

ensure that the Council's vision for the town, as the shareholder, is able to form part of the direction of travel of each company. The Framework also gives assurance that each company is operating in an effective and accountable way.

Annual Review of Effectiveness

Blackpool Council has responsibility for conducting, at least annually, a review of the effectiveness of its governance framework, including the system of internal control. The stages included in the review process and the key findings from each are summarised below.

Annual Governance Statement Review Group

An Annual Governance Statement Review Group was established in February 2016 and has led on the review of effectiveness and the production of the Annual Governance Statement, including reviewing the 2014/15 statement to ensure that governance issues identified have subsequently been addressed. This group comprised of the Chief Internal Auditor, Director of Governance and Partnerships, Head of Democratic Governance and Head of Corporate Development, Engagement and Communications.

Elected Member Workshop

A workshop was held on the 15th March 2016 with representation from the Audit Committee, Scrutiny Committee, Standards Committee and Cabinet and facilitated by the Chief Internal Auditor, Head of Democratic Governance and Head of Corporate Development, Engagement and Communications.

The workshop was based around the principles of good governance and elected members were asked to establish what arrangements are already in place and these have been reflected in the overview of the governance framework included in this report. Elected members were also asked to identify areas for further development and these have been incorporated into the significant governance issues action plan.

Key Officer Workshop

A workshop was held on the 25th April 2016 with key officers involved in governance. This included the Chief Internal Auditor, Director of Governance and Partnerships, Head of Democratic Governance, Head of Organisation and Workforce Development, Head of ICT, Chief Accountant and Corporate Development Manager.

The workshop was based around the principles of good governance and an assessment was made as to what controls already form part of the Council's governance framework and also areas which needed further development. This process identified a number of areas of good practice and these have been summarised in the governance framework outlined earlier in this report and areas for improvement have been captured in the significant governance issues action plan.

Annual Governance Statement 2015/2016

Control Self-Assessment Questionnaire

The Corporate Leadership Team was required to complete a control self-assessment questionnaire providing assurance that their directorates were compliant with a number of key controls. Each Director was asked to highlight the three most significant control issues faced over the next twelve months and the risks have been incorporated into the significant governance issues action plan.

Assurance Statement

The results of the effectiveness of the governance framework have been considered by the Corporate Leadership Team and Audit Committee who have determined that the arrangements are fit for purpose in accordance with the governance framework.

Significant Governance Issues

Actions have been identified as part of the 2015/16 review of the effectiveness of the governance framework and these are captured in the following table. It should be noted that some of the issues identified are not deemed as significant but have been included to aid openness and transparency.

Issue	Actions	Responsible Officer
Further embed arrangements in place relating to conduct and behaviours to raise awareness and ensure compliance.	Raise awareness of the whistleblowing policy to employees, elected members and the public.	Chief Executive
	Further promote the Council's values and embed the Leadership Charter.	
	Review the Ethical Principles to ensure that they remain fit for purpose.	
The Council needs to review the way in which it consults with residents and ensures that data collected through the consultation process is adequately considered.	When implementing different approaches to engage with the community, such as the Council Couch, there is a need to ensure that elected members are appropriately consulted with and that senior managers engage in the process.	Chief Executive
	The data which the Council collates in relation to the thoughts of the community should be more effectively used to inform decisions relating to service delivery.	
	New ways to consult with residents who do not ordinarily engage in consultation exercises should be	

Annual Governance Statement 2015/2016

Issue	Actions	Responsible Officer
	<p>considered and there is a need to ensure that consultation exercises are appropriately timed.</p> <p>Improved coordination with partner organisations in relation to data collection could better inform service delivery decisions and avoid potential duplication in consultation processes.</p> <p>Assess the data which the Council makes available to the community to ensure that it contains an appropriate level of detail and is presented in an accessible way.</p>	
<p>Performance management should be more robust and the data more accessible.</p>	<p>There is a need to review the performance data available to the community to ensure that it is relevant, understandable and empowers residents.</p> <p>The process for setting performance targets should be improved and there is a need to strengthen appropriate intervention in cases of low performance where outcomes may not be achieved.</p> <p>The Delivery Unit should be implemented to ensure services deliver appropriate outcomes and improve the quality of performance management data.</p> <p>The Policy Framework should be reviewed to ensure that all appropriate policies and strategies are in place and any gaps are addressed.</p>	<p>Chief Executive</p>
<p>Corporate Policies and Procedures need to be consistently applied.</p>	<p>There is a need to raise awareness of the Corporate Policies and Procedures in place and ensure that all members of the Senior Leadership Team are compliant.</p> <p>As the Council continue to transform there is a need to ensure that adequate internal controls are maintained, particularly as there is an increasing move to self-service and reduced resources results in less capacity to maintain controls.</p> <p>Workforce planning needs to more closely aligned to the business planning process to ensure that workforce pressures are effectively managed and the Council can</p>	<p>Chief Executive</p>

Annual Governance Statement 2015/2016

Issue	Actions	Responsible Officer
	continue to deliver its statutory duties.	
It is increasingly challenging to set a legal budget due to the austerity measures faced by the Council.	The Corporate Leadership Team need to ensure effective monitoring of the achievement of saving and income targets and balance this with demand pressure for services.	Director of Resources
	Effective financial administration needs to be consistently applied across all services including the accurate and timely raising of sundry debt and the prompt payment of creditor invoices.	
Continue to develop and strengthen the challenge to governance arrangements by the Audit Committee.	Consider the benefits of introducing the role of an independent member, with relevant skills and experience, to be represented on the Audit Committee.	Director of Governance and Partnerships
Effectively manage risk with reduced resources and ensure that risk management is built into all decisions as the climate for taking riskier decisions grows.	The Senior Leadership Team need to consider risk management in the context of opportunity in order to transform the way in which the Council delivers its services.	Chief Executive
	The Senior Leadership Team need to ensure that risk management is embedded into in all decisions taken.	
Ensure that all elected members feel empowered when carrying out these duties.	Enhance the development programme for elected members to ensure that they have the appropriate skills and knowledge to empower them to carry out their duties.	Director of Governance and Partnerships
	Raise Elected Members awareness of the policies and procedures in place which enable all members the opportunity to scrutinise, challenge and contribute to the Council's activities.	

Conclusion

We propose over the coming year to take steps to address the significant governance issues identified to further enhance governance arrangements. We are satisfied that these steps will address the need for improvements that were identified in our review of effectiveness and will monitor their implementation and operation as part of our next annual review.

Annual Governance Statement 2015/2016

Signed: _____ (Leader of the Council)

Signed: _____ (Chief Executive)

This page is intentionally left blank

Report to:	AUDIT COMMITTEE
Relevant Officer:	Iain Leviston, Manager, KPMG
Date of Meeting:	30 June 2016

KPMG TECHNICAL UPDATE

1.0 Purpose of the report:

- 1.1 To consider KPMG's report providing an overview on progress in delivering its responsibilities as the external auditors. The report also highlights the main technical issues that are currently having an impact in local government.

2.0 Recommendation(s):

- 2.1 To note the report and raise any questions and make any recommendations as considered appropriate.

3.0 Reasons for recommendation(s):

- 3.1 To enable the Committee to consider an overview of KPMG's progress in delivering its responsibilities as the external auditors and the main technical issues that are currently having an impact in local government.

3.2a Is the recommendation contrary to a plan or strategy adopted or approved by the Council? No

3.2b Is the recommendation in accordance with the Council's approved budget? Yes

- 3.3 Other alternative options to be considered:

None

4.0 Council Priority:

- 4.1 The relevant Council Priorities are

"The economy: Maximising growth and opportunity across Blackpool"

"Communities: Creating stronger communities and increasing resilience"

5.0 Background Information

5.1 This report builds on the Global Audit campaign ‘Value of Audit: Shaping the future of Corporate Reporting’, to look more closely at the issue of public trust in national governments and how the audit profession needs to adapt to rebuild this trust. The objective is to articulate a clear opinion on the challenges and concepts critical to the value of audit in government today and in the future and how governments must respond in order to succeed.

5.2 Through interviews with KPMG partners from nine countries as well as some senior government audit clients from Canada, the Netherlands and the US, a number of challenges and concepts have been identified that are critical to the value of audit in government today and in the future.

5.3 Does the information submitted include any exempt information? No

5.4 **List of Appendices:**
Appendix 6a: Technical update

6.0 Legal considerations:

6.1 None.

7.0 Human Resources considerations:

7.1 None.

8.0 Equalities considerations:

8.1 None

9.0 Financial considerations:

9.1 See attached report.

10.0 Risk management considerations:

10.1 None

11.0 Ethical considerations:

11.1 None

12.0 Internal/ External Consultation undertaken:

12.1 See attached report.

13.0 Background papers:

13.1 None

This page is intentionally left blank



Technical update

Contents

The contacts at KPMG in connection with this report are:

Trevor Rees
Director
KPMG LLP (UK)
Tel: 0161 246 4063
trevor.rees@kpmg.co.uk

Iain Leviston
Manager
KPMG LLP (UK)
Tel: 0161 246 4314
iain.leviston@kpmg.co.uk

KPMG resources


Technical update

Page


3

8

This report provides the audit committee with an overview on progress in delivering our responsibilities as your external auditors. The report also highlights the main technical issues which are currently having an impact in local government. If you require any additional information regarding the issues included within this report, please contact a member of the audit team. We have flagged the articles that we believe will have an impact at the Authority and given our perspective on the issue:

 High impact

 Medium impact

 Low impact

 For information



KPMG resources

Local government budget survey

KPMG has recently published the results of its Local Government Budget Survey. The survey collated data from 97 KPMG local authority clients on topics including:

- The content of budget monitoring reports;
- Savings plans;
- Invest-to-save projects
- The type of savings being made;
- Assumptions underlying the medium term financial plan; and
- Reserve movements.

The Survey also poses questions for management and Members to consider when reviewing their budget setting and budget monitoring processes.

For more information, and a copy of the report, please contact Iain Leviston, whose details can be found on page 2 of this document.

Publication 'Value of Audit - Perspectives for Government'

What does this report address?

This report builds on the Global Audit campaign – *Value of Audit: Shaping the future of Corporate Reporting* – to look more closely at the issue of public trust in national governments and how the audit profession needs to adapt to rebuild this trust. Our objective is to articulate a clear opinion on the challenges and concepts critical to the value of audit in government today and in the future and how governments must respond in order to succeed.

Through interviews with KPMG partners from nine countries (Australia, Canada, France, Germany, Japan, the Netherlands, South Africa, the UK and the US) as well as some of our senior government audit clients from Canada, the Netherlands and the US, we have identified a number of challenges and concepts that are critical to the value of audit in government today and in the future.

What are the key issues?

- The lack of consistent accounting standards around the world and the impacts on the usefulness of government financial statements.
- The importance of trust and independence of government across different markets.
- How government audits can provide accountability thereby enhancing the government's controls and instigating decision-making.
- The importance of technology integration and the issues that need to be addressed for successful implementation
- The degree of reliance on government financial reports as a result of differing approaches to conducting government audits

The *Value of Audit: Perspectives for Government* report can be found on the KPMG website at <https://home.kpmg.com/xx/en/home/insights.html>

The *Value of Audit: Shaping the Future of Corporate Reporting* can be found on the KPMG website at www.kpmg.com/sg/en/topics/value-of-audit/Pages/default.aspx

Publication 'Reimagine - Local Government'

KPMG have published a number of reports under the headline of *Reimagine – Local Government*. These are summarised below:

Council cash crunch: New approach needed to find fresh income

- By 2020, councils must generate all revenue locally.
- More and more are looking towards diversifying income streams as an integral part of this.
- Councils have significant advantages in becoming a trusted, independent supplier.
- To succeed, they must invest in developing commercial capability and capacity.

Councils can save more than cash by sharing data

- Better data sharing in the public sector can save lives and money.
- The duty to share information can be as important as the duty to protect it.
- Local authorities are yet to realise the full value of their data and are wary of sharing information.
- Cross-sector structures and the right leadership is the first step to combating the problem.

English devolution: Chancellor aims for faster and more radical change

- Experience of Greater Manchester has shown importance of strong leadership.
- Devolution in areas like criminal justice will help address complex social problems.
- Making councils responsible for raising budgets locally shows the radical nature of these changes.
- Cuts to business rates will stiffen the funding challenge, even for the most dynamic councils.

Senior public sector pensions

- Recent changes to pensions taxation have particularly affected the public sector, with fears senior staff may quit as pension allowances bite.
- 'Analyse, control, engage' is the bedrock of an effective strategy.

Time for the Care Act to deliver

- Momentum behind last year's Care Act risks stalling.
- Councils are struggling to create an accessible care market with well-informed consumers.
- Local authorities must improve digital presence and engage providers.
- Austerity need not be an impediment to progress. It could be an enabler.

The publications can be found on the KPMG website <https://home.kpmg.com/uk/en/home/insights/2016/04/reimagine-local-government.html>

Publication 'The future of cities'

We are delighted to share *The future of cities*, a report that helps local government leaders build and evaluate sustainable cities for their current and future generations.

What is *The future of cities*?

The future of cities is a global report that follows from the UK firm's thought leadership partnership with the City of Bristol and the work surrounding its European Green Capital 2015 designation. The report is broken into two modules that draw on the expertise of KPMG practitioners around the world and includes a range of case studies to ensure you find approaches relevant to your context.

The first module, *The future of cities: creating a vision*, explains the central role of vision in the success of second cities, identifying seven guiding principles to make cities more attractive. Examples are provided of various cities around the globe that are putting some of these principles into action.

The second, *The future of cities: measuring sustainability*, discusses some of the ways in which cities are being measured and how these metrics could evolve. More important, it provides practical examples of what leading cities are doing, the lessons to be learned and how these can be applied to other cities.

This content is now featured on kpmg.com/futurecities where readers can access a broader collection of reports and shorter opinion pieces from KPMG's leading thinkers on different aspects on how to create better, more sustainable places to live and work.

Page 55



Technical developments

New local audit framework

Level of impact: ● (Medium)	KPMG perspective
<p>The <i>Local Audit and Accountability Act 2014</i> included transitional arrangements covering the audit contracts originally let by the Audit Commission in 2012 and 2014. These contracts covered the audit of accounts up to 2016/17, and gave the Department for Communities and Local Government (DCLG) the power to extend these contracts to 2019/20.</p> <p>DCLG have now announced that the audit contracts for principal local government bodies (including district, unitary and county councils, police and fire bodies, transport bodies, combined authorities and national parks) will be extended to include the audit of the 2017/18 financial statements. From 2018/19, local government bodies will need to appoint their own auditors; currently, there is nothing definite in place whether there will be a sector-led body that is able to undertake this role on behalf of bodies. However the Local Government Association (LGA) has been seeking views and expressions of interest to gauge the appetite in the sector for this approach.</p> <p>CIPFA have now issued guidance that was commissioned by DCLG on the creation of Auditor Panels. The guidance is available at www.cipfa.org/policy-and-guidance/publications/g/guide-to-auditor-panels-pdf. The guidance provides options on establishing an Auditor Panel, and the roles and responsibilities the panels will have once established.</p> <p>NHS and smaller local government bodies (town and parish councils, and internal drainage boards), will not have their contracts extended, and will have to appoint their own auditors for 2017/18, one year earlier than for larger local government bodies.</p>	<p><i>Members may wish to discuss the options open to them on how to procure their auditor for 2018/19 and beyond and ensure they formulate a timetable for making this decision.</i></p>

Page 57

Modern Slavery Act 2015

Level of impact: ● (Medium)	KPMG perspective
<p>The <i>Modern Slavery Act 2015</i> has now been enacted.</p> <p>All organisations, including local authorities / public bodies, with a year end on or after 31 March 2016 and a turnover greater than £36m have to produce a statement about the current financial year setting out what steps they have taken to ensure that slavery or human trafficking is not occurring in their supply chain or in their own organisation.</p> <p>All local authorities should already be considering what needs to be done to ensure compliance.</p> <p>Background</p> <p>The Act introduces the concept of 'transparency in supply chains' and requires all commercial organisations which carry on a business in the UK with a total annual turnover of at least £36 million to produce an annual slavery and human trafficking statement. Local authorities satisfy the definition of 'commercial organisations' set out in the Act, so many will be caught.</p> <p>A supply chain includes both direct and indirect suppliers and is very wide ranging including outsourced services supplied by agencies. Local authorities need to be satisfied that modern slavery does not exist at any point in the chain leading to a good or service supplied to them.</p> <p>Examples of suppliers where risks may exist across all departments are:</p> <ul style="list-style-type: none">— firms engaged to build / refurbish public buildings / areas;— agencies supplying cleaners; and— suppliers of repair / maintenance materials and / or services. <p>As recent cases in the media demonstrate, modern slavery is not something occurring solely outside the UK and the implications both reputationally and legally can be significant.</p>	<p><i>The Committee may wish to seek assurances how their Authority is progressing with the new requirements.</i></p>

Modern Slavery Act 2015 (cont.)

Page 59

What should the statement include?

The statement must set out what steps the organisation has taken during the financial year to ensure that slavery and human trafficking is not occurring either in your supply chain or within your own organisation. Although a statement could simply be made saying no steps have been taken in relation to slavery and human trafficking, the legislation suggests the statement should cover the following:

- The organisation's structure, business and supply chains;
- Its policies in relation to slavery and human trafficking;
- Its due diligence processes in relation to slavery and human trafficking;

The parts of its business and supply chain where there is a risk of slavery and human trafficking taking place and the steps it has taken to assess and manage that risk;

Its effectiveness in ensuring that slavery and human trafficking is not taking place in its business or supply chain measured against appropriate performance indicators;

The training and capacity building about slavery and human trafficking available to its staff.

The statement needs to be approved and published on the website, with a link in a prominent place on the website's home page. The statement should be published within six months of the financial year end.

There are no financial or criminal penalties for failing to produce a statement, although the Secretary of State may seek an injunction through the High Court requiring the organisation to comply. However, the reputational damage an organisation may suffer if it chooses not to report or to take no action may be significant.

What should local authorities be doing?

There is obviously a lot for local authorities to consider in order to be able to publish their first statement relating to the current financial year. In preparation they should be considering what type of statement they want to make, who will be responsible for compliance, how they identify and assess the risks of slavery and trafficking in their supply chain and how they determine the level of due diligence that needs to be undertaken, what policies and training is going to be put in place and how they are going to ensure effective ongoing monitoring and review. But the clock is ticking and time is running out.....

For further information or if you would like us to come out and see you to discuss how the Modern Slavery Act could impact the Authority please contact Julie Bruce (Julie.bruce@kpmg.co.uk) (0115 935 3420) or your local KPMG contact

CIPFA/LASAAC briefing on Highway Network Assets

Level of impact: ● (Medium)	KPMG perspective
<p>Authorities will be aware that the CIPFA/LASAAC consultation on the Draft Code of Practice on the Highways Network Asset (HNA Code) closed in April 2016.</p> <p>Following the consultation, the second in a series of Briefings on the Highways Network Asset has been made available on the CIPFA website at: http://www.cipfa.org/policy-and-guidance/local-authority-highways-network-asset.</p> <p>The Briefing covers the HNA Code consultation, the definition of the Highways Network Asset, 2015/16 reporting requirements and the Central Assurance process.</p> <p>Further guidance, and future briefings, on this topic are also available on this same webpage.</p>	<p><i>The Committee may wish to understand the progress their Authority has made in its plans to meet the new reporting requirements.</i></p>

Page 60

Exercising electors' rights - 2015/16 changes

Level of impact: ● (Low)	KPMG perspective
<p>Authorities may be aware that the <i>Accounts & Audit Regulations 2015</i> have introduced new arrangements for the exercise of electors' rights, which take effect from the 2015/16 financial statements. One of the most significant changes is that the auditor is no longer required to 'call the audit' and specify a date upon which electors can meet with the auditor and ask questions about the accounts.</p> <p>Regulation 15 requires the Responsible Financial Officer (RFO), after signing and dating the draft accounts on behalf of the Authority, to commence the period for the exercise of electors' rights. This period is limited to 30 working days, and for 2015/16 must include the first 10 working days of July.</p> <p>Authorities should also note that Regulation 9(2) is clear that the authority's meeting to consider and approve the accounts should take place after the period for the exercise of electors' rights has ended. Due to the requirement in Regulation 15 for a common inspection period during July, the inspection period this year cannot end before 14 July 2016. This means that authorities should not approve and publish their accounts before 15 July 2016.</p> <p>Electors' rights are important, and the courts have in the past been critical of those who have not ensured that adequate provision for the exercise of these rights is made.</p> <p>Auditors are mindful that they may be contacted by electors or their representatives during the 30 working day inspection period. Given the limited time available, auditors will ensure that they have adequate arrangements in place during the prescribed period for receiving and identifying promptly whether any correspondence received includes formal questions under the <i>Local Audit and Accountability Act 2014</i>, and/or objections to the accounts.</p>	<p><i>The Committee may wish to seek assurances that the impact for their Authority is understood.</i></p>

Councillors' travel expenses

Level of impact: ● (Low)	KPMG perspective
<p>HM Revenue and Customs (HMRC) are in the process of contacting Local Authorities to commence PAYE and NIC compliance reviews focusing on the historic treatment of councillors' mileage expenses. Those authorities that are unable to demonstrate they have reported payments correctly face a tax and NIC charge, with interest and potentially penalties applying.</p> <p>The previous rules</p> <p>Up until 5 April 2016, HMRC could agree that for some councillors, home is a place of work and therefore the cost of journeys to council offices could be paid free of tax and NIC. This could have been the case where, for example, councillors were required to see constituents at home. HMRC do not accept however that working from home out of choice makes home a place of work and in these cases, any expenses reimbursed in respect of travel to council offices should have been subject to tax and NIC.</p> <p>HMRC Compliance Reviews</p> <p>Those local authorities that are unable to support their historic treatment of councillor mileage expenses face a liability to unpaid PAYE, NIC, interest and potentially penalties going back four, and possibly six years. It will be important for local authorities to review their expenses records to determine how travel expenses have been treated and the processes and rationale behind that treatment. Given that different councillors can have different working patterns it will be important to review the treatment on a case by case basis.</p> <p>The new rules</p> <p>With effect from 6 April 2016, a new exemption has been introduced for councillors' travel expenses. From this date, a councillor's journey between their home and their office will be treated as 'business travel' which means that any mileage expenses reimbursed for this journey will, up to certain limits, be free of tax and NIC (subject to their home not being more than 20 miles outside the relevant authority boundary).</p> <p>How KPMG can help</p> <p>KPMG's public sector Employment Tax specialists provide practical advice on dealing with HMRC Employer Compliance reviews. We regularly assist local authorities in liaising with HMRC and staying ahead of legislative and practice developments. If you would like to speak to one of our specialists please contact your normal KPMG contact.</p>	<p><i>The Committee may wish to seek assurances how their Authority is progressing with the new requirements.</i></p>

Capital receipts flexibility

Level of impact: ● (Low)	KPMG perspective
<p>The 2015 Spending Review included an announcement that local authorities would be able to use capital receipts on the revenue costs of service reform projects. The Department for Communities and Local Government (DCLG) has now issued guidance on the capital receipts flexibility, including a draft direction setting out the types of project that would qualify and expected governance and transparency framework. In summary:</p> <ul style="list-style-type: none">— the flexibility is available from 1 April 2016 to 31 March 2019;— only capital receipts generated during that period can be used for the flexibility;— the Secretary of State's direction will have the effect of allowing authorities to treat revenue expenditure on service reform as capital during the three year period;— authorities will not be allowed to borrow to fund revenue expenditure on service reform; and— authorities are required to have regard to a statutory code which contains certain transparency requirements when taking advantage of the flexibility. <p>We understand that DCLG's aim is that the final signed direction will be issued with the final settlement in February 2016.</p> <p>A copy of the draft guidance can be found at www.gov.uk/government/uploads/system/uploads/attachment_data/file/486999/Capital_receipts_flexibility_-_draft_statutory_guidance_and_direction.pdf</p>	<p><i>The Committee may wish to seek assurances how their Authority is planning to use the new flexibility.</i></p>

Page 63

Better Care Fund policy framework 2016/17

Level of impact: ● (Low)	KPMG perspective
<p>The Department of Health, in conjunction with the Department for Communities and Local Government, has recently published 2016/17 Better Care Fund planning guidance.</p> <p>The guidance introduces a number of changes, requiring local clinical commissioning groups (CCGs), councils and providers to establish risk sharing arrangements to fund unplanned emergency admissions. Local areas will also have to agree to 'stretching' local targets for cutting delayed transfers of care supported by an action plan.</p> <p>The guidance can be found here: www.gov.uk/government/publications/better-care-fund-how-it-will-work-in-2016-to-2017</p>	<p><i>The Committee may wish to seek assurances how their Authority is developing these arrangements.</i></p>

Page 64

2015/16 Code of Practice Update

Level of impact: ● (Low)	KPMG perspective
<p>CIPFA/LASAAC has issued an update to the <i>2015/16 Code of Practice on Local Authority Accounting in the United Kingdom</i> (the Code) following its consultation process. The 2015/16 Code update should be read alongside the 2015/16 Code published in April 2015.</p> <p>Authorities should note that the update confirms the transitional reporting requirements for the measurement of the Highways Network Asset. The Code does not require a change to the preceding year information for the move to measuring the Highways Network Asset at current value (and under that provision would not require a change to the balance sheet information at 1 April 2015). It also does not require a restatement of the opening 1 April 2016 information but there will need to be an adjustment to those balances.</p> <p>The Code update also includes amendments as a result of legislative changes and particularly the <i>Accounts and Audit Regulations 2015</i> for English authorities. It specifies the principles for narrative reporting which CIPFA/LASAAC considers should be used to meet the new requirements of those regulations.</p>	<p><i>The Committee may wish to seek assurances that their Authority is aware of the update to the 2015/16 Code</i></p>

Page 65

NAO report 'English devolution deals'

Level of impact: ● (For Information)

Published on 20 April, this report finds that devolution deals to devolve power from central government to local areas in England offer opportunities to stimulate economic growth and reform public services for local users, but the arrangements are untested and government could do more to provide confidence that these deals will achieve the benefits intended.

The report is available free of charge and the full version or a summary can be accessed at <https://www.nao.org.uk/report/english-devolution-deals/>

Greater Manchester Combined Authority'

Level of impact: ● (For Information)

Greater Manchester Combined Authority (GMCA) has pioneered the concept of local devolution within England. 'Devo Manc' encompasses a broad range of proposals to address the challenges and opportunities GM is facing:

Health and Social Care

Greater Manchester is facing an estimated financial deficit of c. £2 billion by 2020/21. A Memorandum of Understanding was signed in February 2015 between all partners in GM, committing the region to produce a comprehensive Strategic and sustainable Plan for health and social care.

As part of the Plan, GM is seeking to use its share of the £8 billion promised to the NHS in the CSR to support new recurrent costs and protect social care budgets, closing over a quarter of the funding gap. A further investment by the partners of £500 million, phased over three years, will release future recurrent savings with a likely payback of £3 for every £1 invested.

GM proposals

In addition, GM has made a number of proposals to reform the way public services work together and deliver services within the region:

- Investment in transport infrastructure
- Research and innovation funding
- New funding mechanisms to support site remediation and infrastructure provision
- Investment in integrated business support to drive growth and productivity
- Making better use of Social Housing Assets to support growth
- Reform of the New Homes Bonus
- Locally led low carbon
- Further employment and skills reform
- A scaled-up GM Reform Investment Fund
- GM approach to data sharing across public agencies
- Devolution of decision making for apprenticeships and training, and reform to careers advice and guidance
- Fiscal devolution, including reform to Business Rates, Council Tax, Stamp Duty Land Tax and a Hotel Bed Tax
- Fundamental review of the way services to children are delivered

All of these proposals involve joint working, not just with other GM agencies, but also central government departments. This allows the existing financial resources provided to the region to be redeployed more efficiently to maximise the benefits to GM.

Proposed changes to business rates and core grants

Level of impact: ● (For Information)

The Chancellor of the Exchequer has proposed some radical reforms of local government finance. The proposals are that by the end of the decade, councils will retain all locally raised business rates but will cease to receive core grant from Whitehall.

Under the proposals, authorities will be able to keep all the business rates that they collect from local businesses, meaning that power over £26 billion of revenue from business rates will be devolved.

The uniform national business rate will be abolished, although only to allow all authorities the power to cut rates. Cities that choose to move to systems of combined authorities with directly elected city wide mayors will be able to increase rates for specific major infrastructure projects, up to a cap, likely to be set at £0.02 on the rate.

The system of tariffs and top-ups designed to support areas with lower levels of business activity will be maintained in its present state.

'Cities and Local Government Devolution Act 2016'

Level of impact: ● (For Information)

Authorities will wish to note that the *Cities and Local Government Devolution Act 2016* received Royal Assent on 28 January 2016. The Act provides the enabling legislation to:

- allow for the election of mayors for a combined authority area;
- allow for the devolution of functions, including transport, health, skills, planning and job support; and
- provide a power to establish sub-national transport bodies which will advise the Government on strategic schemes and investment priorities in their own area.

Most of the changes under the Act, including the implementation of 'devolution' deals, will be implemented by Orders to be made under the Act.



© 2016 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

Report to:	AUDIT COMMITTEE
Relevant Officer:	Tracy Greenhalgh – Chief Internal Auditor
Date of Decision/ Meeting	30 June 2016

STRATEGIC RISK REGISTER

1.0 Purpose of the report:

- 1.1 To consider the Council’s revised Strategic Risk Register.
- 1.2 The Strategic Risk Register was last approved by the Audit Committee on 24 September 2015 and the revised version has been subject to a full review and amended accordingly.

2.0 Recommendation(s):

- 2.1 The Audit Committee is asked to:
- Consider and approve the Strategic Risk Register.
 - Consider continuing to call risk owners to future meetings to discuss progress against addressing each risk.

3.0 Reasons for recommendation(s):

- 3.1 Blackpool Council’s Risk Management Framework 2014-2017 was agreed by Audit Committee on the 24 April 2014. This sets out the roles and responsibilities of the Audit Committee and these include:

- Monitor the adequacy of the Council’s risk management arrangements.
- Approve the strategic risk register developed by officers and consider progress reports on the risks included in it.
- Provide assurance on behalf of the Council about the extent to which risk management objectives are being met.
- Approve the Council’s Risk Management Framework.

3.2a Is the recommendation contrary to a plan or strategy adopted or approved by the Council? No

3.2b Is the recommendation in accordance with the Council’s approved budget? Yes

3.3 Other alternative options to be considered:
None.

4.0 Council Priority:

4.1 The relevant Council Priorities are:

“The economy: Maximising growth and opportunity across Blackpool”
“Communities: Creating stronger communities and increasing resilience”

5.0 Background Information

5.1 The Strategic Risk Register is reviewed and updated by the Corporate Risk Management Group and the Corporate Leadership Team. It receives annual approval from the Audit Committee and Risk Owners are required to attend Audit Committee on a periodic basis to provide an update in terms of how each risk is being managed.

5.2 The Strategic Risk Register was last approved by the Audit Committee on the 24 September 2015 and has recently been updated by the Corporate Risk Management Group at a meeting on the 26 April 2016.

5.3 The Strategic Risk Register is split into two key documents:

- The first of these is the Strategic Risk Register Summary that provides an overview in relation to the current risk categories, associated risks, net risk score, the number of controls which need to be implemented to mitigate the risk and the CLT Lead.
- The second document is the detailed Strategic Risk Register which will be used by the Corporate Risk Management Group to ensure that actions are addressed and the summary sheet can be updated as appropriate.

Does the information submitted include any exempt information? No

List of Appendices:

Appendix 7a – Strategic Risk Register Summary
Appendix 7b – Detailed Strategic Risk Register

6.0 Legal considerations:

6.1 The Council needs to ensure that it effectively manages its risks to avoid the potential of legal challenge or prosecution.

7.0 Human Resources considerations:

- 7.1 The actions identified in the Strategic Risk Register will be delivered using existing staffing levels.
- 8.0 Equalities considerations:**
 - 8.1 None.
- 9.0 Financial considerations:**
 - 9.1 Where possible risks will be managed within current budgets. Where it is not feasible to do so this will be escalated to the Corporate Risk Management Group and the Corporate Leadership Team where a decision will be made to accept the risk or identify additional funding to implement the required controls.
- 10.0 Risk management considerations:**
 - 10.1 The Strategic Risk Register is a key component of the Council's overall Risk Management Framework.
- 11.0 Ethical considerations:**
 - 11.1 None.
- 12.0 Internal/ External Consultation undertaken:**
 - 12.1 The Strategic Risk Register has been prepared in consultation with the Corporate Risk Management Group and the Corporate Leadership Team.
- 13.0 Background papers:**
 - 13.1 Risk Management Framework 2014 to 2017.

This page is intentionally left blank

Strategic Risk Register Summary and Monitoring Sheet

No	Risk	Sub No.	Sub-Risk	Nett Risk Score	Additional Mitigations to be Implemented	CLT Risk Owner
1	Lack of Resilience	1a	Lack of individual resilience to work in a changing environment.	12	1	Chief Executive
		1b	Lack of capacity to deliver Council services.	16	2	Chief Executive
					1	Director of People
		1c	Over reliance on public sector services.	16	2	Chief Executive
2	Service Failure	2a	Failure of a service provider in high risk contracted areas such as social care and waste management.	16	1	Director of Resources
		2b	Loss of key infrastructure which results in Council services not being delivered such as ICT and property.	12	3	Director of Resources
3	Sustainability of the Council	3a	Insufficient funding to deliver services.	16	2	Director of Resources
		3b	Further devolution of services and increased partnership working.	16	1	Director of Governance and Partnerships
		3c	Insufficient central government funding for new burdens in social care.	15	2	Director of People
		3d	Unmanageable levels of insurance claims relating to abuse / negligence.	16	1	Director of People
4	Failure the Keep People Safe	4a	Death, serious injury or harm of a vulnerable adult / child.	15	1	Director of People
		4b	Death or injury to a member of staff or the public	15	2	Director of Resources
5	Inadequate Change Management	5a	Unpredictability of legal rulings requiring and unexpected change.	16	1	Director of Governance and Partnerships
		5b	Unfunded new burdens which the Council is required to deliver.	16	1	Chief Executive
6	Reputational Damage	6a	Ineffective measurement of the reputation of the Council and Blackpool.	12	1	Chief Executive
		6b	Negative image of Blackpool to residents	12	2	Chief Executive
		6c	Negative image of Blackpool to visitors.	12	1	Director of Place
7	Ineffective Governance	7a	Non-compliance with statutory requirements and internal procedures.	12	1	Director of Governance and Partnerships
					1	Chief Executive
		7b	Lack of effective risk management embedded across the Council.	12	1	Director of Resource
		7c	Increased risk of fraud.	15	2	Director of Resources
		7d	Data theft and leakage.	12	3	Director of Resource
		7e	Cyber Threat - Phishing e-mails	20	2	Director of Resource
	7f	Cyber Threat - Distributed Denial of Service Attack	10	1	Director of Resource	
8	Unsustainable Local Economy / Increased Deprivation	8a	Lack of affordable housing.	12	1	Director of Place
		8b	Increased deprivation and unemployment.	12	1	Director of Place
					1	Director of Resource
8c	Lack of appropriate highways infrastructure.	12	1	Director of Community and Environment		
9	Inability to Respond to a Major Incident	9a	Reduced capacity across the Council to respond to an emergency.	16	3	Director of Resource
		9b	Injury / death to members of the public or staff.	16	1	Director of People

This page is intentionally left blank

Detailed Strategic Risk Register

No	Risk	Sub No.	Sub-Risk	Impact / Consequences	Opportunity	Gross Risk Score			Controls and Mitigation	Net Risk Score			New / Developing Controls	Risk Manager	CLT Risk Owner	Target Date	Corporate Priority
						I	L	GS		I	L	NS					
1	Lack of Resilience	1a	Lack of individual resilience to work in a changing environment.	Workplace stress.		4	4	16	Health and safety arrangement for managing work related pressure, supported by an online stress work tool.	4	3	12	Robust workforce planning.	Head of Organisation and Workforce Development	Chief Executive	Ongoing	Organisational Resilience
				Decreased staff morale.			A range of training courses in place to help build individual resilience skills.										
						Absence management procedures in place.											
						Workforce planning iPool module in place.											
						People Strategy in place.											
						Access to an employee assistance programme.											
		1b	Lack of capacity to deliver Council services.	Inability to deliver an effective service.	Employee commitment.	4	5	20	Development programmes implemented such as coaching, mentoring and aspiring managers programme.	4	4	16	Effective people planning with a view to more generic roles to reduce the burden on key officers.	Head of Organisation and Workforce Development	Chief Executive	Ongoing	Organisational Resilience
					Unable to recruit into difficult to recruit roles.	Change organisation form / increase joint working arrangements to deliver services with reduced resource.	Development programmes for specific areas of recruitment problems such as social care and teaching.										
					Loss of corporate memory.	Manage relationships with the Trade Unions in order to embrace employee change.	Deliver a programme of commissioning / service reviews to explore alternative delivery models.										
1c	Over reliance on public sector services.	Unable to deliver core services / statutory duties to residents.	Build a more resilient community to reduce reliance on the public sector.	4	5	20	Five Year Council Plan in place.	4	4	16	Delivery and implementation of the Council Plan.	Head of Corporate Development, Engagement and Communication	Chief Executive	Ongoing	Communities		
				Implementation of a robust performance management framework to ensure adequacy of internal service provision.													
2	Service Failure	2a	Failure of a service provider in high risk contracted areas such as social care and waste management.	Increased costs.		5	4	20	4	4	16	Ensure adequate business continuity plans are in place with service providers as part of the procurement and contract management process.	Head of Procurement and Development	Director of Resources	Ongoing	Communities	
				Reputational damage to the Council.													Procurement procedures in place which cover business continuity arrangements.
		2b	Loss of key infrastructure which results in Council services not being delivered such as ICT and Property.	Inability to deliver critical services.	Build a resilient organisation.	5	4	20	Business continuity programme in place.	4	3	12	Ensure all services have up to date business continuity plans in place.	Chief Internal Auditor	Director of Resources	Ongoing	Organisational Resilience
			Corporate business continuity plan in place supported by a critical activity list.	Develop a corporate / thematic business continuity plan for property.	Head of Property and Asset Management	Director of Resources	Ongoing										
			Corporate ICT business continuity guidance in place.	Look for provisions for data centre refresh in the coming years to continue to provide resilience.	Head of ICT Services	Director of Resources	Ongoing										

Detailed Strategic Risk Register

No	Risk	Sub No.	Sub-Risk	Impact / Consequences	Opportunity	Gross Risk Score			Controls and Mitigation	Net Risk Score			New / Developing Controls	Risk Manager	CLT Risk Owner	Target Date	Corporate Priority
						I	L	GS		I	L	NS					
3	Sustainability of the Council	3a	Insufficient funding to deliver services.	Erosion of reserves.	Income generation opportunities.	5	5	25	Downsizing of the Council to meet budget constraints.	4	4	16	Ongoing financial modelling to assess the impact of funding cuts. Unplanned in-year budget cuts such as for Public Health services which need to be addressed plus future significant cuts proposed.	Chief Accountant	Director of Resources	Ongoing	Organisational Resilience
				Priority led budgeting process.					Medium term financial strategy in place.								
			Unplanned overspends.	Monthly financial monitoring including achievement of saving targets and collection of income.	Robust reporting of recovery plans to Scrutiny Committee.												
		3b	Further devolution of services and increased partnership working.	Increased financial risk.		5	4	20	Effective relationships with partners / external agencies.	4	4	16	Ensure robust governance arrangements are in place for new working arrangements.	Head of Demographic Governance	Director of Governance and Partnerships	Ongoing	Organisational Resilience
3c	Insufficient central government funding for new burdens in Adult Social Care in addition to current constraints on cash limited budgets.	Council unable to balance budget.	Council unable to meet statutory duties and deliver reforms.	Consider options for shared services and opportunities for flexible use of new funding streams.	5	4	20	Robust budgetary control mechanisms.	5	3	15	Participate in financial modelling exercises to challenge government assumptions and support lobbying for resource.	Director of Adult Services	Director of People	Ongoing	Organisational Resilience	
			External care market becomes unsustainable					Member led priority based budgeting and financial planning.				Actively participate in system transformation planning with Health					
3d	Unmanageable level of insurance claims relating to historic abuse / negligence in children's social care.	Unplanned overspends.		5	4	25	External legal advice sourced to ensure appropriate expertise.	4	4	16	Review of insurance coverage and excess on this type of claim; training to be provided on how to mitigate the risks going forward.	Deputy Director of Children's Services	Director of People	Ongoing	Organisational Resilience		
4	Failure to Keep People Safe	4a	Death, serious injury or harm of a vulnerable adult / child.	Inspection failure (Ofsted / CCQ).		5	5	25	Safeguarding processes and procedures.	5	3	15	Review all safeguarding procedures and constant auditing.	Director of Adult Services / Deputy Director of Children's Services	Director of People	Ongoing	Communities
				Trauma for family of the victim.					Training and professional development.								
			Potential criminal charges for staff involved.					Contract monitoring.									
			Significant liability claim received.					Risk assessments.									
4b	Death or injury to a member of staff or the public.	Trauma for family of the victim.		5	5	25	Full suite of health and safety arrangements and guidance notes available on the Hub.	5	3	15	Addition of health and safety roles and responsibilities in job descriptions.	Chief Internal Auditor	Director of Resources	Ongoing	Communities		
							Programme of health and safety management system audits in place.				Support and assistance from CLT to embed the monitoring process.						
		Corporate manslaughter changes, prosecution with unlimited fines and potential prison sentences for those in control.					Suite of health and safety training available for all employees.										
		Civil compensation claims.					Team of qualified health and safety professionals.										
		Reputational damage.															
5	Inadequate Change Management	5a	Unpredictability of legal rulings requiring an unexpected change.	Inability to effectively adapt to the required change.		5	4	20	Anticipation work to assess potential impacts.	4	4	16	Oversight of legal rulings which may have an impact on the Council.	Chief Corporate Solicitor	Director of Governance and Partnerships	Ongoing	Organisational Resilience
								Use of court appeals process when appropriate to do so.									

Detailed Strategic Risk Register

No	Risk	Sub No.	Sub-Risk	Impact / Consequences	Opportunity	Gross Risk Score			Controls and Mitigation	Net Risk Score			New / Developing Controls	Risk Manager	CLT Risk Owner	Target Date	Corporate Priority
						I	L	GS		I	L	NS					
		5b	Unfunded new burdens which the Council is required to deliver.	Increased financial obligations. Policy decisions create expectations for residents.		5	4	20	Analysis of previous patterns and trends.	4	4	16	Policy research to identify and communicate potential trends.	Head of Corporate Development, Communication and Engagement	Chief Executive	Ongoing	Organisational Resilience
6	Reputational Damage	6a	Ineffective measurement of the reputation of the Council and Blackpool.	Perception of poor reputation is not quantified / supported.	Rebuilding reputation can suggest a high achieving organisation and generate momentum.	4	4	16	Daily summary of media interest in Blackpool circulated.	4	3	12	Continue to liaise with the media to present positive news stories about Blackpool.	Head of Corporate Development, Communication and Engagement	Chief Executive	Ongoing	Communities and Economy
		6b	Residents negative image of Blackpool.	Lack of investment due to poor image of Blackpool.	Potential to attract external investment to Blackpool.	4	4	16	Different methods of engagement used such as the Council Couch.	4	3	12	Implement corporate framework for engagement supported by an engagement toolkit.	Head of Corporate Development, Communication and Engagement	Chief Executive	Ongoing	Communities and Economy
				Lack of partner engagement.	Generate local pride in Blackpool.				Increased use of new communication channels such as social media and newsletters.				Implementation of the Corporate Branding toolkit.				
6c	Visitors negative image of Blackpool.	Local economy impacted due to reduced jobs. Inability to underwrite tourism initiatives due to reduced resources.		4	4	16	Identification of potential external funding streams to assist with the tourism offer for Blackpool.	4	3	12	Promote a positive image of Blackpool to encourage private sector investment in the tourism industry.	Head of Visitor Economy	Director of Place	Ongoing	Communities and Economy		
7	Ineffective Governance	7a	Non-compliance with statutory requirements and internal procedures.	External challenge.		4	5	20	Statutory legal and financial officers in place.	3	4	12	Raise awareness of standards / required and awareness of the consequence of failure.	Head of Demographic Governance	Director of Governance and Partnerships	Ongoing	Organisational Resilience
				Quality of service compromised.					Policy team research / proactive consultation response.				Consistent use of disciplinary / capability procedures across the Council for serious instances on non-compliance.				
									Assurance mechanisms such as internal audit, external audit, peer review and external assessments.								
								Constitution and Financial Regulations in place.									
								Disciplinary procedures in place.									
		7b	Lack of effective risk management embedded across the Council.	Ineffective decision making.	Potential to make savings through effectively managing risks.	5	4	20	Risk management framework and toolkit in place.	4	3	12	Revisit each risk management group to ensure that it is working effectively and following the requirements of the risk management framework.	Chief Internal Auditor	Director of Resources	Ongoing	Organisational Resilience
				Increased insurance claims.					Service and strategic level risk registers in place.								
								Departmental and thematic risk management groups in place.									
								Risk management consider as part of decision making process.									
		7c	Increased risk of fraud.	Erosion of internal controls and less resource to tackle fraud.	Increased use of Proceeds of Crime Act.	5	4	20	Anti-fraud and corruption policy in place.	5	3	15	Focus on high risk areas of fraud.	Chief Internal Auditor	Director of Resources	Ongoing	Organisational Resilience
									Annual internal audit plan in place.				Increase fraud awareness training Council wide.				

Detailed Strategic Risk Register

No	Risk	Sub No.	Sub-Risk	Impact / Consequences	Opportunity	Gross Risk Score			Controls and Mitigation	Net Risk Score			New / Developing Controls	Risk Manager	CLT Risk Owner	Target Date	Corporate Priority
						I	L	GS		I	L	NS					
		7d	Data theft and leakage.	Significant fines from the Information Commissioner.	The serious nature of the risk and its consequences will encourage departments to work with ICT to implement robust processes.	4	5	20	Working with services to undertake risk assessments against the Information Asset Register to identify opportunities to identify areas where effort must be focused to reduce the likelihood of a data breach.	4	3	12	Ensure documents and equipment are disposed of appropriately as part of the programme of office moves.	Head of ICT Services	Director of Resources	Ongoing	Organisational Resilience
						Data risk assessments.				Promotion and adoption of data risk assessments.							
										Continued development of robust processes regarding starters / leavers and retrieval of kit.							
		7e	Cyber Threat - Phishing E-mails.	Fraud	Improve knowledge and awareness across departments on identifying phishing emails. Report anything that is opened.	5	5	25	Investing in Sandbox technology.	4	5	20	Continue to develop and refine technologies to provide proactive altering and monitoring of the changing threats.	Head of ICT Services	Director of Resources	Ongoing	Organisational Resilience
				Reputational damage.	Participate in training and knowledge gathering opportunities.				Investigating in SEIM (Security Information Event Management) to proactively monitor activity on the network.				Review use of white listing to mitigate risk of being hijacked and introduce SPF (Sender Policy Framework) to check against spoofing.				
				Loss of compliance. Monetary penalties / fines.					Increase cyber defences and use blacklist / reputation to authenticate email.								
		7f	Cyber Threat - Distributed Denial of Service Attack	Issues with access to the Council website and also potentially the Council network overwhelming the network with unwanted traffic.		5	3	15	Watching what other organisations do to combat the threat.	5	2	10	Continue to investigate enterprise products that combat the issue (however these are currently limited in their effectiveness)	Head of ICT Services	Director of Resources	Ongoing	Organisational Resilience
				Loss of confidence in using Council online services including an impact on Channel Shift.	Maintain two internet connections to provide resilience to switch between connections.												
8	Unsustainable Local Economy / Increased Deprivation.	8a	Lack of good quality affordable housing.	Negative impact on local economy.	Key in the regeneration of Blackpool.	4	4	16	ALMO Stock.	4	3	12	Complete the build of the provision of 400 new family homes on the Rigby Road site and progress Queens Park Development.	Strategic Head of Development	Director of Place	Ongoing	Communities and Economy
				Potential criminal activities.	Revitalise areas in the town.				Regulation of private sector / link with RSLs. Creation of Blackpool Housing Company to help transform private sector housing.								
		8b	Increased deprivation and unemployment.	Dependency on Council services.		4	4	16	Introduction of living wage for Council staff and promoting this with contractors.	4	3	12	Delivery of the Framework for Growth and Prosperity.	Strategic Head of Development	Director of Place	Ongoing	Communities and Economy
								Commitment to use local suppliers where possible.				Completion of the Central Business District Project.	Head of Property and Asset Management	Director of Resource	Ongoing		

Detailed Strategic Risk Register

No	Risk	Sub No.	Sub-Risk	Impact / Consequences	Opportunity	Gross Risk Score			Controls and Mitigation	Net Risk Score			New / Developing Controls	Risk Manager	CLT Risk Owner	Target Date	Corporate Priority
						I	L	GS		I	L	NS					
		8c	Lack of appropriate transport infrastructure.	Loss of trade, reputation and confidence from residents.		4	4	16	Road Asset Management Strategy in place.	4	3	12	Appropriate work undertaken to maintain the condition of the highways infrastructure.	Head of Highways and Traffic Services	Director of Community and Environment	Ongoing	Communities and Economy
9	Inability to Respond to a Major Incident.	9a	Reduced capacity across the Council to respond to an emergency.	May not be able to provide all the resources required as a Category One Responder.	Corporate approach to responding to incidents.	5	4	20	Major Emergency Plan in place outlining roles and responsibilities.	4	4	16	Establish a control centre at Bickerstaff House for dealing with a major incident.	Chief Internal Auditor	Director of Resources	Ongoing	Communities and Economy
				Potential public enquiry if the incident was not dealt with effectively.					Community risk register in place.				Undertake a major incident exercise, as least annually, to ensure that arrangements are adequate.				
				Disruption to community, services and businesses.					Planning for potential incidents through the Lancashire Resilience Forum.				Utilise training opportunities for those involved in dealing with a major incident.				
		9b	Injury / death to members of the public or staff.	Trauma faced by families and work colleagues.		5	4	20	Emergency response group in place to provide humanitarian support in a major emergency.	4	4	16	Maintain the number of volunteers on the emergency response group at adequate levels and attend the Lancashire Resilience Forum Humanitarian Assistance Group.	Director of Adult Services	Director of People	Ongoing	Communities and Economy

This page is intentionally left blank

Report to:	AUDIT COMMITTEE
Relevant Officer:	Tracy Greenhalgh, Chief Internal Auditor
Date of Meeting	30 June 2016

AUDIT COMMITTEE SELF-EVALUATION

1.0 Purpose of the report:

- 1.1 To consider the feedback from the self-evaluation exercise undertaken by the Audit Committee and senior officers who engage with the Committee on a regular basis.

2.0 Recommendation(s):

- 2.1 To consider the outcome of the self-evaluation exercise and determine whether the Committee would like to develop an improvement plan to build on the feedback received.

3.0 Reasons for recommendation(s):

- 3.1 To develop the effectiveness of the Audit Committee.

- 3.2a Is the recommendation contrary to a plan or strategy adopted or approved by the Council? No

- 3.2b Is the recommendation in accordance with the Council's approved budget? Yes

- 3.3 Other alternative options to be considered.
None.

4.0 Council Priority:

- 4.1 The relevant Council Priorities are

“The economy: Maximising growth and opportunity across Blackpool”

“Communities: Creating stronger communities and increasing resilience”

5.0 Background Information

5.1 Elected Member Feedback

5.2 Members of the Audit Committee were invited to complete a self-evaluation checklist to help measure the effectiveness of the Committee. Four Members responded and completed a self-evaluation checklist which was based on the CIPFA Guidance for Audit Committees (2013).

5.3 The self-assessment checklist asked members to consider a number of questions in relation to the following topics:

- Audit Committee Purpose and Governance
- Functions of the Committee
- Membership and Support
- Effectiveness of the Committee

5.4 The results of the completed self-evaluation, along with the results from when the exercise was completed twelve months prior can be seen in the following table. An indication of the direction of travel has also been provided:

Ref	Good Practice Questions	June 2016			June 2015			DoT
		Yes	Partly	No	Yes	Partly	No	
<i>Audit Committee Purpose and Governance</i>								
1	Does the authority have a dedicated Audit Committee?	100%	0%	0%	100%	0%	0%	✓
2	Does the Audit Committee report directly to full Council?	50%	25%	25%	29%	57%	14%	✓
3	Do the terms of reference clearly set out the purpose of the Committee in accordance with CIPFA's Position Statement?	100%	0%	0%	86%	14%	0%	✓
4	Is the role and purpose of the Audit Committee understood and accepted across the authority?	25%	75%	0%	43%	43%	14%	✗
5	Does the Audit Committee provide support to the authority in meeting the requirements of good governance?	100%	0%	0%	86%	14%	0%	✓

6	Are the arrangements to hold the Committee to account for its performance operating satisfactorily?	50%	50%	0%	57%	29%	14%	✗
Functions of the Committee								
7	Does the Committee's term of reference explicitly address all the core areas identified in CIPFA's position statement?							
	• Good governance	100%	0%	0%	86%	14%	0%	✓
	• Assurance framework	75%	25%	0%	86%	14%	0%	✗
	• Internal audit	100%	0%	0%	71%	29%	0%	✓
	• External audit	100%	0%	0%	86%	14%	0%	✓
	• Financial reporting	100%	0%	0%	86%	14%	0%	✓
	• Risk management	75%	25%	0%	86%	14%	0%	✗
	• Value for money or best value	50%	50%	0%	43%	57%	0%	✓
	• Counter-fraud and corruption	100%	0%	0%	86%	14%	0%	✓
8	Is an annual evaluation undertaken to assess whether the Committee is fulfilling its terms of reference and that adequate consideration has been given to all core areas?	75%	25%	0%	57%	14%	29%	✓
9	Has the Audit Committee considered the wider areas identified in CIPFA's Position Statement and whether it would be appropriate for the Committee to undertake them?	25%	75%	0%	14%	72%	14%	✓
10	Where coverage of core areas has been found to be limited, are plans in place to address this?	100%	0%	0%	72%	14%	14%	✓
11	Has the Committee maintained its non-advisory role by not taking on any decision-making powers that are not in line with its core purpose?	75%	25%	0%	100%	0%	0%	✗

Membership and Support								
12	Has an effective Audit Committee structure and composition to the committee been selected? This should include: <ul style="list-style-type: none"> • Separation from the Executive • An appropriate mix of knowledge and skills among the membership • A size of Committee that is not unwieldy • Where independent members are used, that they have been appointed using an appropriate process 	100%	0%	0%	86%	14%	0%	✓
13	Does the Chair of the Committee have appropriate knowledge and skills?	100%	0%	0%	-	-	-	✓
14	Are arrangements in place to support the Committee with briefings and training?	100%	0%	0%	100%	0%	0%	✓
15	Has the membership of the Committee been assessed against the core knowledge and skills framework and found to be satisfactory?	0%	100%	0%	57%	43%	0%	✗
16	Does the Committee have good working relations with key people and organisations, including external audit, internal audit and the Chief Financial Officer?	75%	25%	0%	86%	14%	0%	✗
17	Is adequate secretariat and administrative support to the Committee provided?	100%	0%	0%	100%	0%	0%	✓

Effectiveness of the Committee								
18	Has the Committee obtained feedback on its performance from those interacting with the Committee or relying on its work?	25%	75%	0%	14%	72%	14%	✓
19	Has the Committee evaluated whether and how it is adding value to the organisation?	50%	25%	25%	14%	72%	14%	✓
20	Does the Committee have an action plan to improve any areas of weakness?	50%	25%	25%	29%	42%	29%	✓

5.5 **Officer Feedback**

5.6 A number of Officers who engage with the Audit Committee were also asked to undertake an evaluation of the Committee based on their experiences. A number of questions were asked, based on the CIPFA Guidance on Audit Committees (2013) and officers were also asked to provide any comments or suggestions as to potential improvements going forward. Seven responses were received in total.

5.7 Some officers did not feel that they had enough experience of the Committee to make a judgement and where this is the case the output has been recorded as 'not applicable'.

5.8 The results of the completed self-evaluation, along with the results from when the exercise was completed twelve months prior can be seen in the following table. An indication of the direction of travel has also been provided:

Ref	Good Practice Questions	June 2016			June 2015			DoT
		Yes	Partly	N/a	Yes	Partly	N/a	
1	Is the role and purpose of the Audit Committee understood and accepted across the authority?	71%	29%	0%	60%	40%	0%	✓
2	Does the Audit Committee provide support to the authority in meeting the requirements of good governance?	100%	0%	0%	20%	80%	0%	✓

3	Are the arrangements to hold the Committee to account for its performance operating satisfactorily?	43%	43%	14%	20%	40%	40%	✓
4	Has the Committee maintained its non-advisory role by not taking on any decision-making powers that are not in line with its core purpose?	100%	0%	0%	60%	20%	20%	✓
5	Does the Chair of the Committee have the appropriate knowledge and skills?	100%	0%	0%	-	-	-	✓
6	Does the Committee have good working relations with key people and organisations, including external audit, internal audit and the Chief Financial Officer?	100%	0%	0%	100%	0%	0%	✓
7	Do you consider that the Audit Committee performs well and achieves its core function?	100%	0%	0%	20%	80%	0%	✓
8	Do you believe that the Audit Committee adds value to the organisation?	85%	15%	0%	20%	80%	0%	✓
9	Do you find members of the committee approachable?	100%	0%	0%	100%	0%	0%	✓
10	Do you feel that the committee offers the appropriate level of challenge?	57%	43%	0%	40%	60%	0%	✓

6.0 Comments

6.1 Role and Purpose of Committee

- The role and purpose of the Audit Committee is better understood now that the terms of reference of the Committee have been refined to its core purpose and there is less of a distraction with the finance role.
- The role and purpose of the Committee are well understood at Corporate Leadership Team level; however the level of understanding decreases as the seniority of officers decreases.
- The level of understanding of the role and purpose of the Audit Committee across Elected Members is variable with some having a very good understanding but others requiring further training.

6.2 Committee Performance

- The Chairman takes an active role in the work of the Committee, has a sound level of knowledge and understands the Committee's purpose and direction.
- The Committee has started to add value over the last twelve months and will no doubt build on this in the future.
- Regular training sessions are provided to Committee members to supplement knowledge and skills.
- There is a stronger, structured interaction with scrutiny and also an annual report to Council.
- The introduction of the Chairman's annual report to Council will help hold the Committee to account for its performance. However, it will probably take a while before the Committee's performance is properly challenged via this arrangement.

6.3 Working Relationships

- The Committee members are very approachable and supportive as well as professional.
- There are good relations between key officers and members involved with the Committee.
- It is unclear how external audit interacts directly with the Chairman. This may be an area to develop in the future and it may be beneficial to review how this is done in other local authorities.

6.4 Challenge

- As a whole the Committee offers the appropriate level of challenge.
- The challenge role has improved over the last twelve months with the Chairman in particular leading the holding to account process. This has encouraged other members to follow suit, although not all members fully buy into this way of working.

- Having an opposition party member as Chairman of the Committee helps lead the activity. On the whole the Committee operates in a non-political way and seeks to provide the required level of assurance.

Does the information submitted include any exempt information?

No

List of Appendices:

None.

7.0 Legal considerations:

7.1 The purpose of the self-evaluation is to help ensure that Members effectively fulfil their responsibilities as members of the Audit Committee.

8.0 Human Resources considerations:

8.1 Members may wish to complete the CIPFA Guidance on Audit Committees (2013) evaluation titled 'Audit Committee Members – Knowledge and Skills Framework'. This may identify additional training and development needs which could potentially be provided internally, or where budget allows, at external events.

9.0 Equalities considerations:

9.1 All Members of the Committee have the same access to training available.

10.0 Financial considerations:

10.1 It is anticipated that the training programme for Committee Members will be delivered within existing Council budgets.

11.0 Risk management considerations:

11.1 The Audit Committee has a key role in the governance of the Council and therefore it is important that it engages in the development and delivery of an improvement plan to ensure that it can effectively manage risk.

12.0 Ethical considerations:

12.1 None

13.0 Internal/ External Consultation undertaken:

13.1 Consultation has taken place with Members of the Committee and Chief Officers.

14.0 Background papers:

14.1 CIPFA Audit Committee Guidance (2013).

Report to:	AUDIT COMMITTEE
Relevant Officer:	Mark Towers, Director of Governance and Partnerships
Date of Meeting	30 June 2016

REGULATION OF INVESTIGATORY POWERS ACT (2000) POLICY AND PROCEDURE

1.0 Purpose of the report:

1.1 To consider the Regulation of Investigatory Powers Act (2000) (RIPA) policy and procedure.

2.0 Recommendation(s):

2.1 To consider and approve the policy and procedures relating to the Regulation of Investigatory Powers Act (2000).

3.0 Reasons for recommendation(s):

3.1 The Council has had a policy and procedure in place for a number of years, however there has been a need to review the policy and procedures to ensure that they remain relevant.

3.2a Is the recommendation contrary to a plan or strategy adopted or approved by the Council? No

3.2b Is the recommendation in accordance with the Council's approved budget? Yes

3.3 Other alternative options to be considered:

None

4.0 Council Priority:

4.1 The relevant Council Priorities are

“The economy: Maximising growth and opportunity across Blackpool”

“Communities: Creating stronger communities and increasing resilience”

5.0 Background Information

- 5.1 The Regulation of Investigatory Powers Act 2000 regulates covert investigations by various bodies, including local authorities. It was introduced to ensure that individuals' rights are protected whilst ensuring that law enforcement and security agencies have the powers they need to do their job effectively. The Act provides a framework within which activities, which it covers, can be carried out in a manner consistent with the individuals Human Rights. It also provides statutory protection for the authority concerned if its provisions are adhered to.
- 5.2 The purpose of the policy is to:
- Explain the scope of the 2000 Act and where it applies
 - Provide guidance on the internal authorisation procedures to be followed
 - Provide guidance on applications for judicial approval
- 5.3 The Council has had regard to the Codes of Practice produced by the Home Office and the Office of Surveillance Commissioners in preparing this Policy.
- 5.4 The 2000 Act requires that when the Council undertakes "directed surveillance" or uses a "covert human intelligence source" these activities must only be authorised by an officer with delegated powers when the relevant statutory criteria are satisfied.
- 5.5 Authorisation and judicial approval under the 2000 Act gives lawful authority to carry out surveillance and the use of a source. Obtaining authorisation and judicial approval protects the Council and its officers from complaints of interference with the rights protected by Article 8 (1) of the European Convention on Human Rights enshrined in English law through the Human Rights Act 1998.
- 5.6 Provided activities undertaken are also "reasonable and proportionate", they will not be in contravention of Human Rights legislation.

Does the information submitted include any exempt information?

No

List of Appendices:

Appendix 9a – RIPA Policy and Procedure

6.0 Legal considerations:

- 6.1 Non-adherence to the Policy and Procedures could result the Council contravening the Human Rights Act and may prevent the successful prosecutions of those identified as committing criminal activities.

7.0 Human Resources considerations:

7.1 Staff involved in the process are offered the opportunity to attend training on the requirements of RIPA.

8.0 Equalities considerations:

8.1 None.

9.0 Financial considerations:

9.1 The RIPA process is already embedded into the Council's investigatory activities and therefore will not result in an additional cost.

10.0 Risk management considerations:

10.1 There is a risk that the Council is subject to legal action due to non-compliance with the RIPA legislation and Human Rights Act.

11.0 Ethical considerations:

11.1 All applications submitted are assessed to determine whether they are proportionate to the activity taking place and controls implemented to reduce the impact of collateral damage.

12.0 Internal/ External Consultation undertaken:

12.1 The Policy and Procedures have been prepared by the Corporate RIPA Group, which includes representation from Risk Services, Democratic Governance, Legal Services, Human Resources, Public Protection, ICT, Community Safety, CCTV, and Street Cleaning.

13.0 Background papers:

13.1 None.

This page is intentionally left blank

Regulation of Investigatory Powers Act Policy and Guidelines

Blackpool Council



Regulation of Investigatory Powers Act (2000)

Contents

	Page(s)
1. About this document	5
2. Introduction	6 – 7
3. Internal Governance	7 – 9
4. Directed Surveillance	9 – 11
5. Covert Use of Human Intelligence Source (CHIS)	11
6. Authorisations, renewals, duration and judicial approval	11 – 20
7. Specific Areas when RIPA needs to be considered	20 – 21
8. CCTV Systems	21 – 22
9. Social Media	22 – 23
10. Tracking Devices	23
11. 'Drive By' Surveillance	23
12. Noise Monitoring Equipment	23
13. Central Register of Authorisations	24 – 25
14. Retention	25
15. Supporting information, Codes of Practice and Forms	26

Regulation of Investigatory Powers Act (2000)

Appendices

[Appendix 1](#) – Flowchart – Human Rights infringement

[Appendix 2](#) - Home Office Code of Practice - Covert Surveillance and Property Interference

[Appendix 3](#) - Home Office Code of Practice – Covert Human Intelligence Sources

[Appendix 4](#) - Directed Surveillance – Forms and Aides-memoire

- RIP 1 Application for authority for Directed Surveillance
- RIP 2 Supplementary form for all renewals
- RIP 3 Cancellation of directed surveillance
- RIP 4 Review form
- RIP 5 Non-RIPA investigation

[Appendix 5](#) –Covert Human Intelligence Source (CHIS) – Application Forms

- CHIS 1 Application for authority for use of CHIS
- CHIS 2 Cancellation of CHIS
- CHIS 3 Application for renewal of CHIS
- CHIS 4 Review of CHIS authorisation

[Appendix 6](#) -List of Authorised Officers

[Appendix 7](#) -Application for Judicial Approval

[Appendix 8](#) - Home Office guidance to local authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance

[Appendix 9](#) - Home Office Guidance for Magistrates Courts

[Appendix 10](#) - Surveillance Quality Monitoring Form

Regulation of Investigatory Powers Act (2000)

1. About this document

- 1.1 The **Regulation of Investigatory Powers Act 2000** (RIPA) was passed to ensure that various investigatory powers available to public bodies are only exercised in accordance with Human Rights legislation.
- 1.2 The Act envisages three types of surveillance. Each of these has its own authorisation procedure. These classes are:

Directed Surveillance

This is the covert surveillance undertaken in relation to a specific investigation or operation, which is likely to result in the obtaining of private information about someone.

Authorisation for the surveillance can **only** be granted if specific statutory criteria are met and are subject to judicial approval.

Covert Human Intelligence Source

This is where for example an investigating Officer establishes a relationship with a person for the purpose of obtaining information relevant to an investigation without the officer revealing his or her identity.

Similarly, there are statutory criteria, which must be met before authorisation is obtained and judicial approval is required.

Intrusive Surveillance

This is surveillance on or of domestic premises or a private vehicle. Local Authorities are not empowered to carry this out.

- 1.3 This guide tells you more about the permitted types of surveillance and what you must do to obtain the right authorisation AND JUDICIAL APPROVAL.

Remember if in doubt – ALWAYS seek authorisation and judicial approval!

Regulation of Investigatory Powers Act (2000)

2. Introduction

- 2.1 The Regulation of Investigatory Powers Act 2000 (the 2000 Act) as amended regulates covert investigations by various bodies, including local authorities. It was introduced to ensure that individuals' rights are protected whilst ensuring that law enforcement and security agencies have the powers they need to do their job effectively. The Act provides a framework within which activities, which it covers, can be carried out in a manner consistent with the individuals Human Rights. It also provides statutory protection for the authority concerned if its provisions are adhered to.
- 2.2 The Council is therefore included within the 2000 Act framework with regard to the authorisation of both "Directed Surveillance" and of the use of "Covert Human Intelligence Sources".
- 2.3 The purpose of this Policy is to:
- explain the scope of the 2000 Act and where it applies
 - provide guidance on the internal authorisation procedures to be followed
 - provide guidance on applications for judicial approval
- 2.4 The Council has had regard to the Codes of Practice produced by the Home Office and the Office of Surveillance Commissioners in preparing this Policy.
- 2.5 The 2000 Act requires that when the Council undertakes "directed surveillance" or uses a "covert human intelligence source" these activities must only be authorised by an officer with delegated powers when the relevant statutory criteria are satisfied.
- 2.6 Each relevant Director and Deputy Director and the Deputy Chief Executive must nominate officers at Service Manager level or above who can authorise both these activities. Such nomination permits officers to grant authority for any purpose under the terms of the 2000 Act across all Council Directorates and Divisions. (In other words, any Authorising Officer can authorise a surveillance application).
- 2.7 Authorisation and judicial approval under the 2000 Act gives lawful authority to carry out surveillance and the use of a source. Obtaining authorisation and judicial approval protects the Council and its officers from complaints of interference with the rights protected by Article 8 (1) of the European Convention on Human Rights enshrined in English law through the Human Rights Act 1998. This is because the interference with the private life of citizens will be "in accordance with the law".

Regulation of Investigatory Powers Act (2000)

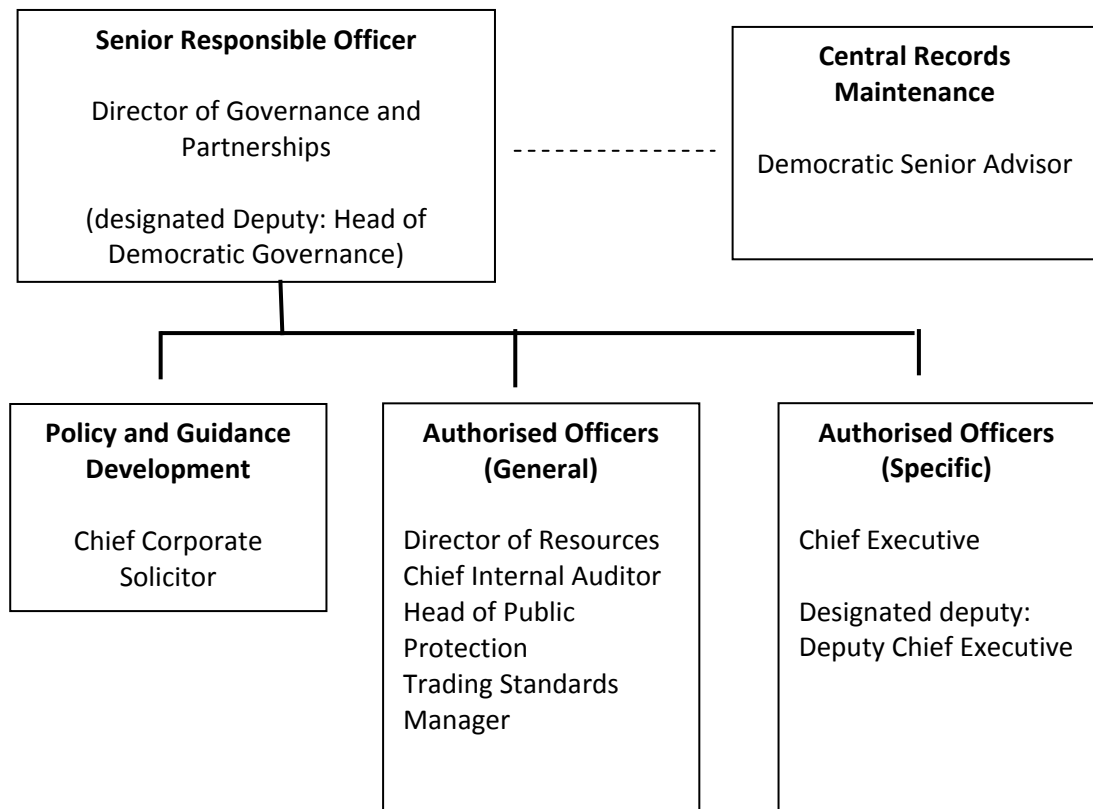
Provided activities undertaken are also “reasonable and proportionate”, they will not be in contravention of Human Rights legislation.

- 2.8 Authorising Officers and investigators within the Local Authority should note that the 2000 Act does not extend powers to conduct Intrusive Surveillance. Investigators should familiarise themselves with the provisions of Sections 4 and 5 of the Code of Practice on directed Surveillance to ensure a good understanding of the limitation of their powers within the 2000 Act.
- 2.9 Deciding when authorisation is required involves making a judgement. Paragraph 4.4 explains this process. If you are in any doubt, seek the advice of an Authorising Officer. If they are in doubt, they will seek advice from the Chief Corporate Solicitor.

Remember - if in doubt – obtain authorisation and judicial approval.

3. Internal Governance

- 3.1 The Council has implemented a governance structure for the RIPA process to ensure that appropriate roles and responsibilities are in place and to enable effective oversight. This is shown in the following structure chart:



Regulation of Investigatory Powers Act (2000)

- 3.2 The role of the Senior Responsible Officer is to oversee the competence of Authorising Officers and the processes in use in by the Council. It is their responsibility to ensure that investigation and enforcement activity are not inadvertently straying into activity that should be, or is capable of being authorised under the Acts. The Senior Responsible Officer cannot authorise RIPA applications, as this would affect their objectivity. In line with best practice, the Senior Responsible Officer is a Chief Officer at the Council.
- 3.3 The Chief Corporate Solicitor is responsible for updating the Policy and Guidance document to ensure that this reflects any changes to legislation, which the Council need to adhere too. To ensure transparency approval of the Policy and Guidance document is sought from both the Corporate Leadership Team and the Audit Committee when significant changes are made. The Chief Corporate Solicitor will also provide advice to Authorised Officers on the application of the Policy and Guidance as and when required.
- 3.4 The role the Authorising Officers is detailed throughout this document. Most authorisations can be carried out by the identified officers, however there are some specific types of authorisation, which need to be undertaken by the Chief Executive (Head of Paid Service) or their designated Deputy (Deputy Chief Executive).
- 3.5 A number of Council employees are able to apply for a RIPA authorisation if necessary to help them undertake their duties. The role of the applicant is to present the facts of the application for covert surveillance:
- The crime to be investigated;
 - The reason why is it proposed to conduct the investigation covertly;
 - What covert tactics are requested and why;
 - Whom the covert surveillance will be focused on;
 - Who else may be affected; and
 - How it is intended to conduct covert surveillance
- 3.6 To assist the Authorising Officers assessment of proportionality, the applicant should provide facts and evidence, but it is not the role of the applicant to establish that it is necessary and proportionate; that is the statutory responsibility of the Authorising Officer.
- 3.7 A Corporate RIPA Group has been established which is represented by all those involved in the governance of RIPA along with other services who can contribute to the discussions such as CCTV, ICT and HR. The group meets at least twice a year, but will meet more frequently when necessary.
- 3.8 The Chief Internal Auditor reports to the Audit Committee on a quarterly basis the number of RIPA applications, which have been authorised in the quarter and a brief summary of the nature of exercise being undertaken.

Regulation of Investigatory Powers Act (2000)

4. Directed Surveillance

4.1 What is meant by Surveillance?

Surveillance includes:

- Monitoring, observing or listening to persons, their movements, their conversations or their other activities or communication
- Recording anything monitored, observed or listened to in the course of surveillance and
- Surveillance by or with the assistance of a surveillance device.

4.2 When is surveillance directed?

Surveillance is “Directed” for the purposes of the 2000 Act if it is covert (but not intrusive) and is undertaken:

- For the purpose of a specific investigation or a specific operation.
- In such a manner as is likely to result in the obtaining of private information about a person (whether or not one is specifically identified for the purpose of the investigation or operation); and
- Otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation to be sought for the carrying out of the surveillance.

4.3 Surveillance becomes intrusive if the covert surveillance

- (i) Is carried out in relation to anything taking place on any “residential premises” or in any “private vehicle”; and
- (ii) Involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device; or
- (iii) Is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle but is carried out without that device being present on the premises or in the vehicle, where the device is such that it consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle. (i.e. remote devices)
- (iv) Additionally directed surveillance on certain premises whilst being used for legal consultation such as solicitors’ offices and courts is to be treated as intrusive. If in doubt, seek advice from the Chief Corporate Solicitor.
- (v) The Council is not empowered to carry out intrusive surveillance

Regulation of Investigatory Powers Act (2000)

4.4 Before any Council officer undertakes any surveillance of any individual or individuals, they need to assess whether the activity comes within the 2000 Act. In order to do this the following questions need to be asked.

4.5 Is the surveillance covert?

Covert surveillance is that carried out in a manner calculated to ensure that subjects of it are unaware it is or may be taking place.

If activities are open and not hidden from the subjects of an investigation, the 2000 Act framework does not apply.

4.6 Is it for the purposes of a specific investigation or a specific operation?

For example, are CCTV cameras, which are readily visible to anyone, covered? The answer is not if their usage is to be monitoring the general activities of what is happening in the area of coverage. If that usage, however, changes, the 2000 Act may apply.

For example, if the CCTV cameras are targeting a particular known individual, and are being used in monitoring his or her activities, that will amount to a specific operation, which will require authorisation.

Please note that such usage of the CCTV system is prohibited unless a valid RIPA authorisation that has been judicially approved is in force.

4.7 Is it in such a manner that is likely to result in the obtaining or private information about a person?

“Private information” is any information relating to a person’s private or family life. If it is likely that observations will not result in the obtaining of private information about a person, then it is outside the 2000 Act framework. However, the use of “test purchasers” may involve the use of “covert human intelligence sources” (see below).

4.8 What about an immediate response to event or circumstances where it is not reasonably practicable to get authorisation?

The Home Office gives the example of an immediate response to something happening during the course of an observer’s work, which is not foreseeable. However, if, as a result of an immediate response, a specific investigation subsequently takes place that brings it within the 2000 Act framework.

Regulation of Investigatory Powers Act (2000)

5. Covert use of Human Intelligence Source (CHIS)

5.1 A person is a Covert Human Intelligence Source if:

- (i) They establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph b) or c)
- (ii) They covertly uses such a relationship to obtain information or provide access to any information to another person; or
- (iii) They covertly disclose information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.
- (iv) A purpose is covert, in relation to the establishment of maintenance of a personal or other relationship, if the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of that purpose.
- (v) It is not clear from the Act whether information should be confined to private information alone. The inference is there, but it is not expressly stated.

If in doubt, obtain authorisation and judicial approval.

6. Authorisations, renewals, duration and judicial approval

6.1 The Conditions for Authorisation

Directed Surveillance

6.1.1 For directed surveillance, no officer shall grant an authorisation for the carrying out of directed surveillance unless they believe:

- (i) That an authorisation is necessary (on the grounds detailed below) and
- (ii) The authorised surveillance is proportionate to what is sought to be achieved by carrying it out.

Grounds: An authorisation is necessary if it is necessary for the purpose of preventing or detecting crime or of preventing disorder.

6.1.2 Additionally, authorisation may not be granted unless:

- (i) It is for the purpose of preventing or detecting conduct which:
 - (a) constitutes one or more criminal offences; or
 - (b) Is / or corresponds to any conduct which, if it all took place in England and Wales, would constitute one or more criminal offences.

And

Regulation of Investigatory Powers Act (2000)

- (ii) The criminal offence or one of the criminal offences referred to is or would be
 - (a) an offence which is punishable, whether on summary conviction or on indictment, by a maximum term of at least 6 months of imprisonment; or
 - (b) an offence under:
 - s146 Licensing Act 2003 (sale of alcohol to children)
 - s147 Licensing Act 2003 (allowing the sale of alcohol to children)
 - s147A Licensing Act 2003 (persistently selling alcohol to children)
 - s7 Children and Young Persons Act 1933 (sale of tobacco etc. to persons under eighteen)

It is, therefore, essential that Investigators consider the offence and the penalty attached before considering whether it may be possible to obtain an authorisation.

6.1.3 The onus is therefore on the person authorising such surveillance to satisfy themselves that it is:

- (i) Necessary
- (ii) Proportionate
- (iii) Within the provisions of the 2000 Act.

6.1.4 When assessing proportionality the following elements need to have been evidenced:

- Balancing the size and scope of the operation against the gravity and extent of the perceived mischief;
- Explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others;
- That the activity is an appropriate use of the legislation and the only reasonable way, having considered all others, of obtaining the necessary result; and
- Providing evidence of other methods considered and why they were not implemented.

6.1.5 In order to ensure that Authorising Officers have sufficient information to make an informed decision it is important that detailed records are maintained. As such, the forms in the appendices are to be completed as relevant.

6.1.6 It is also sensible to make any authorisation sufficiently wide to cover all the means required as well as being able to prove effective monitoring of what is done against what is authorised.

Regulation of Investigatory Powers Act (2000)

- 6.1.7 An Authorising Officer would be expected to consider an application, unless they are too ill to give attention, on annual leave, is absent from their office and home, or is for some reason not able within a reasonable time to obtain access to a secure telephone or fax machine. Pressure of work is not to be regarded as rendering it impracticable for an Authorising Officer to consider an application.
- 6.1.8 The Council has a list of approved Authorised Officers who are trained in the process. Only these identified employees are able to authorise RIPA applications. To improve independence where possible the application will be authorised by an officer who is not directly involved in the service, however it is appreciated that this is not always achievable and an Authorised Officer is able to authorise forms for their service.
- 6.1.9 Where an authorisation has been granted for directed surveillance, it will not take effect unless and until a Justice of the Peace has made an Order approving the grant of the authorisation. This means that an appropriate application must then be made, usually via Blackpool Magistrates Court.
- 6.1.10 The Justice of the Peace may only give approval if satisfied that, at the time of the grant of the authorisation:
- (i) There were reasonable grounds for believing that the authorisation was necessary for preventing or detecting crime or preventing disorder and that the authorised surveillance is proportionate to what is sought to be achieved by carrying it out.
 - (ii) That the authorisation concerns an appropriate offence.
 - (iii) That the grant of authorisation was by a designated person with appropriate authority and that any other conditions that may be imposed by an Order of the Secretary of State are satisfied.

The above need to be satisfied at the date of the application for approval.

- 6.1.11 If the Justice of the Peace refuses to approve the grant of authorisation, then s/he has power to quash it.

Covert Use of Human Intelligence Sources

- 6.1.12 The activity that may be authorised is any conduct that:
- (i) involves activities, such as the use of covert human intelligence source, as described in the authorisation;
 - (ii) consists in conduct by or relates to the person who is specified or described as the person to whose actions as a covert human intelligence source the authorisation relates; and

Regulation of Investigatory Powers Act (2000)

- (iii) is carried out for the purposes of, or in connection with, the investigation or operation so specified or described
- (iv) An Authorising Officer will consider whether grant of an authorisation would be necessary and proportionate to the intelligence dividend that it seeks to achieve and is compliant with Human Rights Act Articles 6 and 8.

6.1.13 In order to ensure that authorising officers have sufficient information to make an informed decision it is important that detailed records are maintained. As such, the forms available on the Hub are to be completed as relevant.

6.1.14 It is also sensible to make any authorisation sufficiently wide enough to cover all the means required as well as being able to prove effective monitoring of what is done against what is authorised.

6.1.15 An Authorising Officer may grant an authorisation for the use of CHIS only on the grounds that it is for the prevention or detection of crime or of preventing disorder and if they believe that the use of CHIS is necessary and proportionate. This process is also subject to judicial approval and a Justice of the Peace will need to be satisfied that the requisite tests have been met, namely that at the time of the grant:

- (i) There were reasonable grounds for believing that the authorisation necessary for preventing or detecting crime or preventing disorder;
- (ii) The authorisation was granted by an appropriate person with power to grant the authorisation; and
- (iii) Any conditions provided by an Order of the Secretary of State are satisfied
- (iv) And that the above remain met

6.1.16 The Council may prefer to seek the assistance of the police or another public authority to manage its CHIS. In such a case, a written protocol between the parties should be produced in order to ensure that an identified CHIS is properly managed. In the absence of such an agreement, Blackpool Council must ensure that it meets its statutory responsibilities.

6.2 Requirements of the 2000 Act

6.2.1 Authorisations must be in writing. In the Appendix to this guidance are standard forms, which must be used as well as aides-memoires, which give practical guidance on their completion. Officers must direct their mind to the circumstances of the individual case with which they are dealing when completing the form.

6.2.2 It is acceptable to authorise surveillance against a group or entity involving more than one individual (for example an organised criminal group where only some identifies are known) providing that it is possible to link the individuals to the common criminal purpose being investigated. It is essential to make explicit the reasons why it is necessary and proportionate to include persons, vehicles or other

Regulation of Investigatory Powers Act (2000)

details that are unknown at the time of authorisation, but once identified, they should be added at review. The Authorising Officer should set parameters to limit surveillance and use the review to avoid 'mission creep'.

6.2.3 Although it is possible to combine two authorisations in one form, it is preferable for separate forms to be completed to maintain the distinction between Directed Surveillance and the use of a source.

6.2.4 The key signature on the application is that of the Authorising Officer on the authorisation and this must be handwritten.

6.2.5 Authorising Officers must, when making authorisations, be aware that each authorisation (or renewal of an authorisation) will be subject to judicial approval. The Council will be required to make the application (without giving notice) to a Justice of the Peace.

6.2.6 No activity permitted by an authorisation granted by an Authorising Officer may be undertaken unless and until judicial approval has been obtained.

6.2.7 The Investigator who has been granted an authorisation must make the necessary arrangements for an application for an Order giving judicial approval to the grant to be made via the Magistrates Court. The Authorising Officer and the Investigator may be required to attend before the Justice of the Peace to support the application.

6.2.8 The Justice of the Peace must be provided with a copy of the original RIPA authorisation or notice and supporting documents. This should contain all information that is relied upon. The original RIPA authorisation or notice should be shown to the Justice of the Peace but retained by the Council. The Investigator and/or Authorising Officer must partially complete a form of Application for Judicial Approval. If, unusually, application is made out of hours, two partially completed Applications will be required. The hearing will be in private and evidence will be given on oath.

6.2.9 An authorisation that has been judicially approved will lapse:

- 12 months from date of their grant or from the date of last renewal if it is for the conduct or use of a covert human intelligence source.
- In all other cases (i.e. directed surveillance) three months from the date of their grant or latest renewal.

6.2.10 If, during the currency of an authorisation, the Authorising Officer is satisfied that the authorisation is no longer necessary, they must cancel it. It is a statutory requirement that authorisations are cancelled as soon as they are no longer required. When cancelling an authorisation the Authorising Officer should:

Regulation of Investigatory Powers Act (2000)

- Record the date and times that surveillance took place and the order to cease the activity.
- Record the reason for cancellation.
- Ensure that surveillance equipment has been removed and returned.
- Provide directions for the management of the product.
- Ensure that detail of persons subjected to surveillance is properly recorded.
- Record the value of the surveillance (i.e. whether the objectives as set in the authorisation were met).

6.2.11 In respect of a juvenile or vulnerable person, the duration of authorisation is one month only, and it must be granted either by:

- The Chief Executive or in his absence
- The Deputy Chief Executive

6.2.12 Any person entitled to grant a new authorisation can renew an existing authorisation in the same terms at any time before it ceases to have effect if it is considered necessary and proportionate. Regard should be given to factors that may affect the renewal process, for example bank holidays. It should be noted, that reviews and renewals should not broaden the scope of the investigation, but can reduce its terms. When the identities of other criminal associates and vehicle details become known, they should be identified at review and in the renewal authorisation, so long as this is consistent with the terms of the original authorisation. Otherwise, new authorisations are required.

6.2.13 For the conduct of a covert human intelligence source, an Authorised Officer should not renew the CHIS unless a review has been carried out and that person has considered the results of the review when deciding whether to renew or not. A review must cover what use has been made of the source, the tasks given to them and information obtained. **However, all renewals also require judicial approval prior to the expiry of the original authorisation.** The Justice of the Peace will need to be satisfied that a review has been appropriately carried out and will consider the results the review.

Factors to Consider

6.2.14 Any person giving an authorisation should first satisfy themselves that the authorisation is necessary on particular grounds and that the surveillance is proportionate to what it seeks to achieve. Both tests must be considered and satisfied.

6.2.15 Particular consideration should be given to collateral intrusion on or interference with the privacy of persons other than the subject(s) of surveillance.

Regulation of Investigatory Powers Act (2000)

- 6.2.16 An application for an authorisation should include an assessment of the risk of any collateral intrusion or interference. The authorising officer will take this into account, particularly when considering the proportionality of the surveillance.
- 6.2.17 Those carrying out the covert surveillance should inform the Authorising Officer if the operation/investigation unexpectedly interferes with the privacy of individuals who are not the original subjects of the investigation or covered by the authorisation in some other way. In some cases, the original authorisation may not be sufficient and consideration should be given to whether a separate authorisation is required. **Again this would be subject to approval by a Justice of the Peace.**

Home Surveillance

- 6.2.18 The fullest consideration should be given in cases where the subject of the surveillance might reasonably expect a high degree of privacy, for instance at their home, or where there are special sensitivities.

Confidential Material

- 6.2.19 The 2000 Act does not provide any special protection for “confidential material”.

This expression basically covers matters subject to legal professional privilege, confidential, personal or journalistic material. It is further defined in Sections 98 to 100 of the Police Act 1997. Nevertheless, such material is particularly sensitive, and is subject to additional safeguards. In cases where the likely consequence of the conduct of a source would be for any person to acquire knowledge of confidential material, the deployment of the source must be subject to special approval by the Surveillance Commission. A copy of such approval should be provided to the Justice of the Peace in the judicial approval application process. Authorisation can only be granted by the Chief Executive (or the Deputy Chief Executive in their absence) where confidential information or matters subject to legal privilege are likely to be acquired.

- 6.2.20 In general, any application for an authorisation which is likely to result in the acquisition of confidential material should include an assessment of how likely it is that confidential material will be acquired. Special care should be taken where the target of the investigation is likely to be involved in handling confidential material. Such applications should only be considered in exceptional circumstances with full regard to the proportionality issues this raises.
- 6.2.21 The following general principles apply to confidential material acquired under authorisations:
- (i) Those handling material from such operations should be alert to anything that may fall within the definition of confidential material. Where there is

Regulation of Investigatory Powers Act (2000)

- doubt as to whether the material is confidential, advice should be sought from the Chief Corporate Solicitor before further dissemination takes place;
- (ii) Confidential material should not be retained or copied unless it is necessary for a specified purpose;
 - (iii) Confidential material should be disseminated only where an appropriate officer (having sought advice from the Chief Corporate Solicitor) is satisfied that it is necessary for a specific purpose;
 - (iv) The retention or dissemination of such information should be accompanied by a clear warning as to its confidential nature.
 - (v) Confidential material should be destroyed as soon as it is no longer necessary to retain it for a specified purpose.

Combined authorisations

6.2.22 A single authorisation may combine two or more different authorisations under the 2000 Act. Combined authorisations must not include intrusive surveillance activity. . However, the provisions applicable for each of the authorisations must be considered separately by the appropriate authorising officer.

6.2.23 Moreover, judicial approval is required and although it is possible for local authorities to request judicial approval for the use of more than one technique at the same time, in practice, as different considerations need to be applied to different techniques, the Home Office Guidance for Magistrates Courts indicates that it is considered that this would be difficult to perform with the degree of clarity required. This Guidance states that as a rule it is preferable that local authorities should aim to submit separate authorisations or notices to authorise the use of different RIPA techniques.

6.2.24 In cases of joint working, for example, with other agencies on the same operation, authority for directed surveillance must be obtained. However as long as one of the agencies has obtained an appropriate authorisation which shows that joint activity will be conducted and a copy of the authorisation (and any necessary judicial approval) is made available to all relevant parties, this would be compliant. Where Council staff are operating on another agency's authorisation they are to ensure that they are aware as to what activity they are authorised to carry out. The Chief Corporate Solicitor should be informed of the agencies involved and of the officer in charge of the surveillance in such cases of joint working.

Handling and disclosure of material

6.2.25 Authorising Officers are reminded of the guidance relating to the retention and destruction of confidential material as described in paragraph 6.2.21.

6.2.26 Authorising Officers are responsible for ensuring that authorisations undergo timely reviews and are cancelled promptly after directed surveillance activity is no longer necessary.

Regulation of Investigatory Powers Act (2000)

- 6.2.27 Authorising Officers must ensure that the relevant details of each authorisation are sent to the Director of Governance and Partnerships as described in this Policy and Guidelines (Section 13).
- 6.2.28 Applications for directed surveillance should be retained by the Authorising Officer, for a period of five years. Where it is believed that the records could be relevant to pending or future criminal proceedings, they should be retained for a suitable further period, commensurate to any subsequent review.
- 6.2.29 There is nothing in the 2000 Act that prevents material obtained through the proper use of the authorisation procedures from being used in other investigations. However, the use outside the Council, of any material obtained by means of covert surveillance and, other than in pursuance of the grounds on which it was obtained, should be authorised only in the most exceptional circumstances, after consultation with the Chief Corporate Solicitor.

Review and Cancellation of Authorisations

- 6.2.30 Council Officers are reminded of the necessity for Initial Authorisations to include details of proposed review dates for surveillance authorities, and that where it is determined that authorisation is no longer required, a Form of Cancellation is completed, authorised and submitted in accordance with Authorisation procedures.

6.3 The Use of Covert Human Intelligence Sources – Employees

- 6.3.1 The Authorising Officer must consider the safety and welfare of an employee acting as a source, and the foreseeable consequences to others of the tasks they are asked to carry out. A risk assessment should be carried out before authorisation is given. Consideration from the start for the safety and welfare of the employee, even after cancellation of the authorisation, should also be considered.
- 6.3.2 The Authorising Officer must believe that the authorised use of an employee as a source is proportionate to what it seeks to achieve. Accurate and proper records should be kept about the source and tasks undertaken.
- 6.3.3 Before authorising the use of an employee as a source, the Authorising Officer should believe that the conduct/use including the likely degree of intrusion into the privacy of those potentially affected is proportionate to what the use or conduct of the source seeks to achieve. He should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the operation or investigation (collateral intrusion). Measures should be taken, wherever practicable, to avoid unnecessary intrusion into the lives of those not directly connected to the operation.

Regulation of Investigatory Powers Act (2000)

- 6.3.4 Particular care should be taken in circumstances where people would expect a high degree of privacy or where, as a consequence of the authorisation, “confidential material” is likely to be obtained.

7. Specific Areas where RIPA needs to be considered.

Test Purchases

- 7.1 When a young person carries out a test purchase at a shop, they are unlikely to be construed as a CHIS on a single transaction, but this would change if the juvenile revisits the same establishment in a way that encourages familiarity. If covert recording equipment is worn by the test purchaser, it will be desirable to obtain an authorisation for directed surveillance. In all cases, a prior risk assessment is essential in relation to a young person.
- 7.2 When conducting covert test purchase operations at more than one establishment, it is not necessary to construct an authorisation for each premises to be visited but the intelligence must be sufficient to prevent ‘fishing trips’. Premises may be combined within a single authorisation provided that each is identified at the outset. Necessity, proportionality and collateral intrusion must be carefully addressed in relation to each of the premises

Use of EBay

- 7.3 CHIS Authorisation is only required for the use of an internet trading organisation, such as eBay, when a covert relationship is likely to be formed. The used of disguised purchaser details in a simple, overt, electronic purchase does not require a CHIS authorisation, because no relationship is usually established at that stage

Private Information

- 7.4 Section 26(2) RIPA does not differentiate between current and historical surveillance products. Sections 48(2) of RIPA and section 31(2) of RIP(S)A define surveillance as including ‘monitoring, observing or listening’ which all denote present activity; but present monitoring could be of past events or the collation of previously unconnected data. If there is a systematic movement or details of a particular individual with a view to establishing, for example, a lifestyle pattern or relationship, it is processing personal data and therefore capable of being directed surveillance.
- 7.5.1 The checking of CCTV cameras or databases simply to establish events leading to an incidents or crime is not usually directed surveillance; nor is general analysis of data by intelligence staff for predictive purposes (e.g. identifying crime hotspots or analysing trends or identifying criminal associations). However, research or analysis, which is part of focused monitoring or analysis of an individual or group of individuals is capable of being directed surveillance and authorisation may be considered appropriate. When dealing with private information the Investigator should discuss the need for authorisation with an Authorised Officer to assess

Regulation of Investigatory Powers Act (2000)

whether a RIPA application is required. What was discussed and the outcome of this should be evidenced to provide a clear audit trail of the decision making process.

8. CCTV Systems

- 8.1 CCTV systems are normally not within scope of RIPA or RIP(S)A since they are overt and not being used for “a specific operation or investigation” (section 26(2)(a)/1(2)(a), defining directed surveillance). However, the protection afforded by RIPA and RIP(S)A is available when they are used for enforcement activities. In such cases directed surveillance authorisations, setting out what is authorised, how it will be carried out (e.g. which cameras are to be used), and what activity is to be caught and held on the tape or disk that results. Judicial approval will be required. Control room staff should ensure that they understand the terms of the authorisation and Authorising Officers must notify them of any changes.
- 8.2 When CCTV is used covertly, collateral intrusion is inevitable and must be considered by the Authorising Officer with the applicant. This is part of the proportionality test and may lead to refusal or a different approach. The Authorising Officer should examine the product, which should not be made public except so far as it shows the identified target.
- 8.3 Council must ensure that authorisations are properly implemented even when acting on behalf of others, such as the Police, since the product is primarily that of the Council and it may be the Council who receive the complaints or claims in the case of misuse. It is of the utmost importance that any directed surveillance using Council CCTV cameras is properly authorised and judicially approved.
- 8.4 The Council and the Police have protocol and procedures in place to enable the Police to access information from the Council owned CCTV system where appropriate RIPA Authorisations are in place.

9. Social Media

- 9.1 When it is intended to undertake investigations using social media sites, such as Facebook, consideration should be given as to whether there is a need for RIPA authorisation and judicial approval in order to prevent any allegations of unlawfulness. A privacy impact assessment should be undertaken to determine whether the investigation is likely to breach a person’s Article 8 rights.
- 9.2 Surfing publicly available information without gathering, storing or processing material or establishing a relationship, is unlikely to engage Article 8 rights. Therefore, in these instances no authorisation would be required. Surfing as opposed to systematic monitoring of such material is unlikely to infringe into any private sphere. If the latter were proposed to be undertaken then appropriate authorisation and judicial approval should be sought.

Regulation of Investigatory Powers Act (2000)

- 9.3 If a covert Facebook account was created and a 'friend' status requested and granted then a large amount of personal information is likely to become available. Creating a profile and sending a friendship request with a view to obtaining information falls within CHIS conduct and requires an appropriate authorisation and judicial approval. The flowchart at Appendix 1 to this document refers.
- 9.4 It is not unlawful for the Council to set up a false identity but it is inadvisable for an employee of the Council to do so for a covert purpose without authorisation. Using photographs of other persons without their permission to support the false identity infringes other laws. All false identities and the rationale for using them will be reported to and recorded by the Senior Responsible Officer (or their representative) once they have been approved by an Authorising Officer. The Senior Responsible officer will then maintain oversight that these arrangements are appropriate.
- 9.5 The Council will not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without the consent of the person whose identify is used and without considering the protection of that person. The consent must be explicit (i.e. the person from whom consent is sought must agree in writing what is and is not to be done)

10. Tracking Devices

- 10.1 Attaching or placing a tracking device onto, or remotely obtaining information about the location of property, without the consent of the owner when the property is not owned by the Council is property interference, which the Council is not permitted to do.
- 10.2 Placing tracking devices or surveillance equipment in or on vehicles owned by the Council is acceptable. The use of a tracking or recording device is not regarded as covert if the staff using the vehicle or device are appropriately notified that they are in place for the purpose of recording movements or for safety but may also be used for evidential purposes should the need arise. If equipment is issued to a Council employee and used for a purpose not notified to the vehicle occupants this is covert and an appropriate authorisation should be sought. If a device is installed to covertly monitor, record, observe or listen to other occupants and authorisation for directed surveillance is required

11. 'Drive by' Surveillance

- 11.1 If 'Drive by' surveillance is to be undertaken the Investigator should first liaise with an Authorised Officer to assess whether an authorised application is required. Details of this discussion and the outcome should be recorded so that there is a clear audit trail of the decision made.

Regulation of Investigatory Powers Act (2000)

12. Noise Monitoring Equipment

- 12.1 Measuring levels of noise audible in the complainant's premises is not surveillance because the noise has been inflicted by the perpetrator, which has probably forfeited any claim to privacy. Using sensitive equipment to discern speech or other noisy activity not discernible by the unaided ear is covert, likely to obtain private information and may be intrusive surveillance which the Council is not permitted to undertake. Where possible, the intention to monitor noise should be notified to the owner and occupier of the premises being monitored. Where notice is not possible or has not been effective, covert monitoring may be considered necessary and proportionate.

13. Central Register of Authorisations

- 13.1 The 2000 Act requires a central register of all authorisations and judicial approvals to be maintained. The Director of Governance and Partnerships maintains this register
- 13.2 Whenever an authorisation is granted the Authorising Officer must arrange for the following details to be forwarded in hard copy to the Director of Governance and Partnerships. (A electronic version will also be kept on the Z drive).
- Whether it is for Directed Surveillance or CHIS
 - Applicant's name and Job Title (manager responsible)
 - Directorate and Section
 - Applicant's address and Contact Number
 - Title of the investigation or operation with brief description and Identity of "Target"
 - Unique reference number of the investigation/ operation
 - Authorising Officer and Job Title
 - Date of Authorisation
 - Date and Order of Judicial Approval, refusal and/ or quashing as soon as possible after obtained.
 - The information provided should identify whether confidential information is likely to be obtained and whether the authorisation was granted by an individual directly involved in the investigation.
- 13.3 If the authorisation is subsequently renewed or cancelled the following must be provided in hard copy to the Director of Governance and Partnerships
- 13.4 The forms on the Appendices to this Policy must be used at all times.

Regulation of Investigatory Powers Act (2000)

- 13.5 It is each Department's responsibility to forward all applications to the Director of Governance and Partnerships for central storage. Authorisation should only be held for as long as it is necessary. It is the responsibility of the Authorising Officer to notify the Director of Governance and Partnerships, once the investigation is closed (bearing in mind cases may be lodged sometime after the initial work). Upon receipt of this confirmation, both the paper copies and electronic copies of individual applications held centrally should be disposed of in an appropriate manner (e.g. shredded). A log of the application will be maintained on the central register.
- 13.6 It should be noted that all covert activity that is not properly authorised should be reported to the Senior Responsible Officer as soon as it is recognised who will then report this to the Office of Surveillance Commissioners (OSC) in writing. An initial e-mail alerting the OSC will be followed by a report detailing circumstances and remedial action. This does not apply to covert activity, which is deliberately not authorised because an Authorising Officer considers that it does not meet legislative criteria, but allows it to continue. It does including activity which should have been authorised, but was not or which was conducted without the directions provided by the Authorising Officer.
- 13.7 When it is decided to use covert surveillance without the protection of RIPA or RIP(S)A the details should still be reported to the Senior Responsible Officer (or their representative) who will maintain a record of decisions and actions. Such activity will be regularly reviewed by the Senior Responsible Officer.
- 13.8 All surveillance equipment owned by the Council is also logged on a central register maintained by the Governance and Regulatory Service. When applying for authorisation the applicant should cross-reference the equipment deployment records and the relevant authorisation.

14. Retention

- 14.1 It is each Department's responsibility to retain securely all authorisations within their Departments. Those and data obtained as a result of investigations must be stored securely and be accessible to and handled only by officers with appropriate responsibility in the relevant Department. As set out in the Council's Corporate Retention Schedule, authorisations and data will generally be held for six years unless a longer period is required due to their continued materiality in relation to court proceedings.
- 14.2 All records held by the Departments should be disposed of in an appropriate manner (e.g. shredded).
- 14.3 Authorising Officers, through the relevant data controller, should ensure compliance with the appropriate data protection requirements under the Data Protection Act 1998, the Council's Corporate Retention Schedule and the departmental practices is to take place for the secure handling and storage of materials.

Regulation of Investigatory Powers Act (2000)

15. Supporting information, Codes of Practice and Forms

- 15.1 Staff should refer to the Codes of Practice produced in the appendices to this Policy for supplementary guidance.
- 15.2 The relevant Codes of Practice, Forms, and sample completed forms are available in the [RIPA Section of the Council's Intranet \(The Hub\)](#).
- 15.3 Any queries relating to RIPA or this document should be addressed in the first instance to the Chief Corporate Solicitor.

Regulation of Investigatory Powers Act (2000)

Document Control

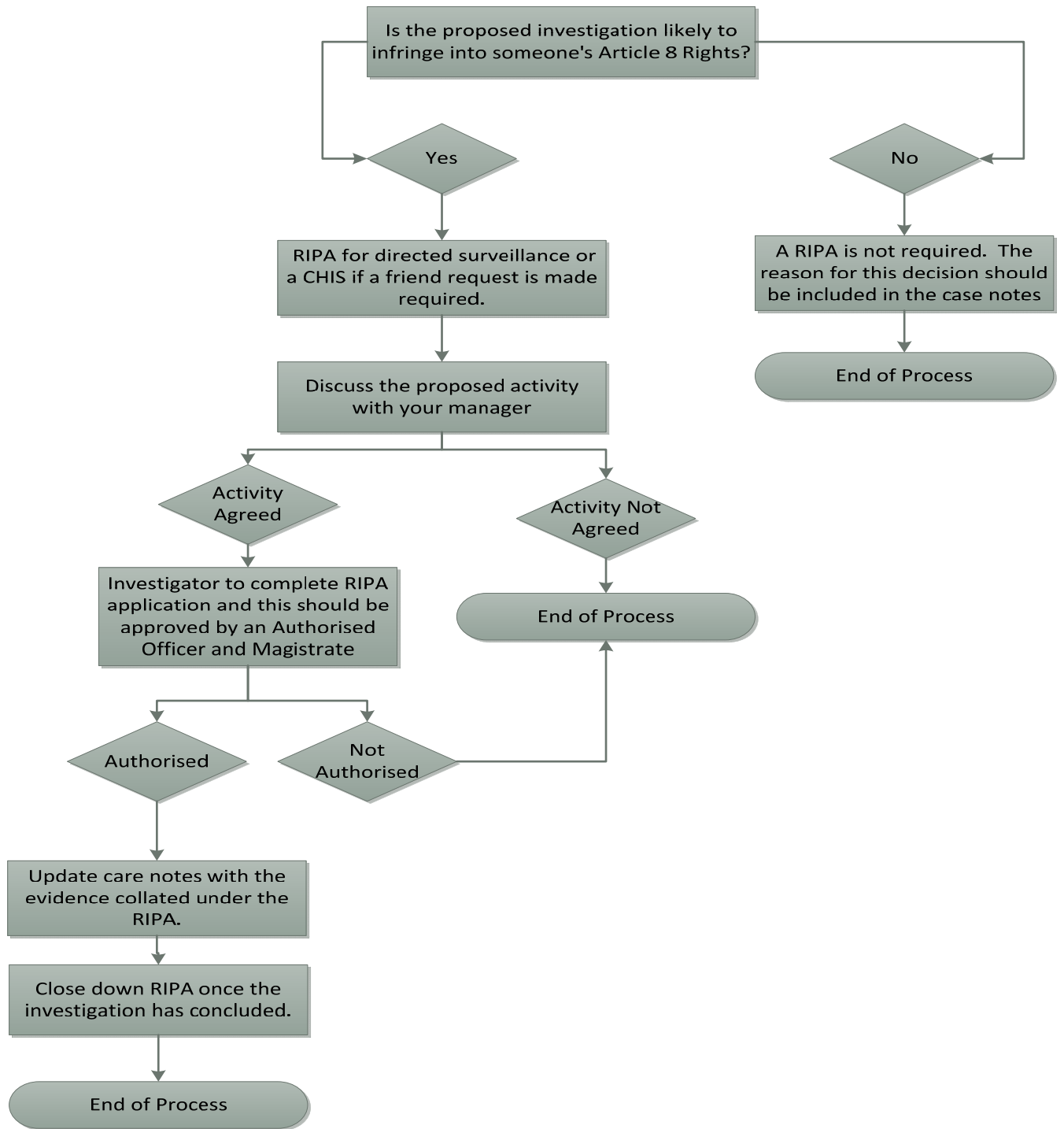
Document owner:	Chief Corporate Solicitor
Document number:	Version 2
Document category:	Policy
Document location:	The Hub
Issued by:	Chief Corporate Solicitor
Last edited:	January 2016

Approved By:

Name	Date
Corporate RIPA Group	
Corporate Leadership Team	
Audit Committee	

Appendix 1

Regulation of Investigatory Powers Act (2000)



Appendix 2



Home Office

Covert Surveillance and Property Interference

Code of Practice

Pursuant to Section 71 of the Regulation of
Investigatory Powers Act 2000

Covert Surveillance and Property Interference

Code of Practice

Pursuant to section 71(4) of the Regulation of
Investigatory Powers Act 2000

LONDON: TSO



information & publishing solutions

Published by TSO (The Stationery Office) and available from:

Online

www.tsoshop.co.uk

Mail, Telephone, Fax & E-mail

TSO

PO Box 29, Norwich, NR3 1GN

Telephone orders/General enquiries:

0870 600 5522

Fax orders: 0870 600 5533

E-mail: customer.services@tso.co.uk

Textphone: 0870 240 3701

TSO@Blackwell and other Accredited Agents

Published with the permission of the Home Office on behalf of the Controller of Her Majesty's Stationery Office.

© Crown Copyright 2014

All rights reserved

You may re-use this information (excluding logos) free of charge in any format or medium, under the terms of the Open Government Licence v.2. To view this licence visit www.nationalarchives.gov.uk/doc/open-government-licence/version/2/ or email PSI@nationalarchives.gsi.gov.uk. Where third-party material has been identified, permission from the respective copyright holder must be sought.

Whilst every attempt has been made to ensure that the information in this publication is up to date at the time of publication, the publisher cannot accept responsibility for any inaccuracies.

First published 2014

ISBN 9780113413737

Printed in the United Kingdom for The Stationery Office.
J002969998 C10 12/14

Contents

Chapter 1	Introduction	5
Chapter 2	Directed and intrusive surveillance definitions	11
Chapter 3	General rules on authorisations	26
Chapter 4	Legally privileged and confidential information	38
Chapter 5	Authorisation procedures for directed surveillance	47
Chapter 6	Authorisation procedures for intrusive surveillance	54
Chapter 7	Authorisation procedures for property interference	64
Chapter 8	Keeping of records	78
Chapter 9	Handling of material and use of material as evidence	81
Chapter 10	Oversight by Commissioners	83
Chapter 11	Complaints	84
Chapter 12	Glossary	85
Annex A	Authorisation levels when knowledge of confidential information is likely to be acquired	88

Chapter 1

INTRODUCTION

Definitions

1.1 In this code:

- ‘1989 Act’ means the Security Service Act 1989;
- ‘1994 Act’ means the Intelligence Services Act 1994;
- ‘1997 Act’ means the Police Act 1997;
- ‘2000 Act’ means the Regulation of Investigatory Powers Act 2000 (RIPA);
- ‘RIP(S)A’ means the Regulation of Investigatory Powers (Scotland) Act 2000;
- ‘2010 Order’ means the Regulation of Investigatory powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010;
- terms in *italics* are defined in the Glossary at the end of this code.

Background

1.2 This code of practice provides guidance on the use by *public authorities* of Part II of the 2000 Act to authorise covert surveillance that is likely to result in the obtaining of *private information* about a person. The code also provides guidance on entry on, or interference with, property or with wireless telegraphy by *public authorities* under section 5 of the Intelligence Services Act 1994 or Part III of the Police Act 1997.

1.3 This code is issued pursuant to section 71 of the 2000 Act, which stipulates that the *Secretary of State* shall issue one or more codes of practice in relation to the powers and duties in Parts I to III of the 2000 Act, section 5 of the 1994 Act and Part III of the 1997 Act. This code replaces the previous code of practice issued in 2010.

1.4 This code is publicly available and should be readily accessible by *members* of any relevant *public authority*¹ seeking to use the 2000 Act to authorise covert surveillance that is likely to result in the obtaining of *private information* about a person or section 5 of the 1994 Act or Part III of the 1997 Act to authorise entry on, or interference with, property or with wireless telegraphy.

1.5 Where covert surveillance activities are unlikely to result in the obtaining of *private information* about a person, or where there is a separate legal basis for such activities, neither the 2000 Act nor this code need apply.²

Effect of code

1.6 The 2000 Act provides that all codes of practice relating to the 2000 Act are admissible as evidence in criminal and civil proceedings. If any provision of this code appears relevant to any court or tribunal considering any such proceedings, or to the Investigatory Powers Tribunal established under the 2000 Act, or to one of the Commissioners responsible for overseeing the powers conferred by the 2000 Act, it must be taken into account. *Public authorities* may also be required to justify, with regard to this code, the use or granting of *authorisations* in general or the failure to use or grant *authorisations* where appropriate.

1.7 Examples are included in this code to assist with the illustration and interpretation of certain provisions. Examples are not provisions of the code, but are included for guidance only. It is not possible for theoretical examples to replicate the level of detail to be found in real cases. Consequently, *authorising officers* should avoid allowing superficial similarities with the examples to determine their decisions and should not seek to justify their decisions solely by reference to the examples rather than to the law, including the provisions of this code.

1 Being those listed under section 30 of the 2000 Act or specified in orders made by the *Secretary of State* under that section.

2 See Chapter 2. It is assumed that intrusive surveillance will always result in the obtaining of *private information*.

Surveillance activity to which this code applies

1.8 Part II of the 2000 Act provides for the *authorisation* of covert surveillance by *public authorities* where that surveillance is likely to result in the obtaining of *private information* about a person.

1.9 Surveillance, for the purpose of the 2000 Act, includes monitoring, observing or listening to persons, their movements, conversations or other activities and communications. It may be conducted with or without the assistance of a surveillance device and includes the recording of any information obtained.³

1.10 Surveillance is covert if, and only if, it is carried out in a manner calculated to ensure that any persons who are subject to the surveillance are unaware that it is or may be taking place.⁴

1.11 Specifically, covert surveillance may be authorised under the 2000 Act if it is either intrusive or directed:

- Intrusive surveillance is covert surveillance that is carried out in relation to anything taking place on residential premises or in any private vehicle (and that involves the presence of an individual on the premises or in the vehicle or is carried out by a means of a surveillance device);⁵
- Directed surveillance is covert surveillance that is not intrusive but is carried out in relation to a specific investigation or operation in such a manner as is likely to result in the obtaining of *private information* about any person (other than by way of an immediate response to events or circumstances such that it is not reasonably practicable to seek *authorisation* under the 2000 Act).

1.12 Chapter 2 of this code provides a fuller description of directed and intrusive surveillance, along with definitions of terms, exceptions and examples.

³ See section 48(2) of the 2000 Act.

⁴ As defined in section 26(9)(a) of the 2000 Act.

⁵ See Chapter 2 for full definition of residential premises and private vehicles, and note that the 2010 Order identified a new category of surveillance to be treated as intrusive surveillance.

Basis for lawful surveillance activity

1.13 The Human Rights Act 1998 gave effect in UK law to the rights set out in the European Convention on Human Rights (ECHR).

Some of these rights are absolute, such as the prohibition on torture, while others are qualified, meaning that it is permissible for the state to interfere with those rights if certain conditions are satisfied.

Amongst the qualified rights is a person's right to respect for their private and family life, home and correspondence, as provided for by Article 8 of the ECHR. It is Article 8 that is most likely to be engaged when *public authorities* seek to obtain *private information* about a person by means of covert surveillance. Article 6 of the ECHR, the right to a fair trial, is also relevant where a prosecution follows the use of covert techniques, particularly where the prosecution seek to protect the use of those techniques through public interest immunity procedures.

1.14 Part II of the 2000 Act provides a statutory framework under which covert surveillance activity can be authorised and conducted compatibly with Article 8. Where covert surveillance would not be likely to result in the obtaining of any *private information* about a person, no interference with Article 8 rights occurs and an *authorisation* under the 2000 Act is therefore not appropriate.

1.15 Similarly, an *authorisation* under the 2000 Act is not required if a *public authority* has another clear legal basis for conducting covert surveillance likely to result in the obtaining of *private information* about a person. For example the Police and Criminal Evidence Act 1984⁶ provides a legal basis for the police covertly to record images of a suspect for the purposes of identification and obtaining certain evidence.

1.16 Chapter 2 of this code provides further guidance on what constitutes *private information* and examples of activity for which *authorisations* under Part II of the 2000 Act are or are not required.

6 See also the Police & Criminal Evidence (Northern Ireland) Order 1989.

Relevant public authorities

1.17 Only certain *public authorities* may apply for *authorisations* under the 2000, 1997 or 1994 Acts:

- Directed surveillance *applications* may only be made by those *public authorities* listed in or added to Part I and Part II of schedule 1 of the 2000 Act.
- Intrusive surveillance *applications* may only be made by those *public authorities* listed in or added to section 32(6) of the 2000 Act, or by those *public authorities* listed in or designated under section 41(1) of the 2000 Act.
- *Applications* to enter on, or interfere with, property or with wireless telegraphy may only be made (under Part III of the 1997 Act) by those *public authorities* listed in or added to section 93(5) of the 1997 Act; or (under section 5 of the 1994 Act) by the intelligence services.

Scotland

1.18 Where all the conduct authorised is likely to take place in Scotland, *authorisations* should be granted under RIP(S)A, unless:

- the *authorisation* is to be granted or renewed (by any relevant *public authority*) for the purposes of national security or the economic well-being of the UK;
- the *authorisation* is being obtained by, or authorises conduct by or on behalf of, those *public authorities* listed in section 46(3) of the 2000 Act and the Regulation of Investigatory Powers (*Authorisations Extending to Scotland*) Order 2000; SI No. 2418); or,
- the *authorisation* authorises conduct that is surveillance by virtue of section 48(4) of the 2000 Act.

1.19 This code of practice is extended to Scotland in relation to *authorisations* granted under Part II of the 2000 Act which apply to Scotland. A separate code of practice applies in relation to *authorisations* granted under RIP(S)A.

International considerations

1.20 *Authorisations* under the 2000 Act can be given for surveillance both inside and outside the UK. However, *authorisations* for actions outside the UK can usually only validate them for the purposes of UK law. Where action in another country is contemplated, the laws of the relevant country must also be considered.

1.21 *Public authorities* are therefore advised to seek *authorisations* under the 2000 Act for directed or intrusive surveillance operations outside the UK if the subject of investigation is a UK national or is likely to become the subject of criminal or civil proceedings in the UK, or if the operation is likely to affect a UK national or give rise to material likely to be used in evidence before a UK court.

1.22 *Authorisations* under the 2000 Act are appropriate for all directed and intrusive surveillance operations in overseas areas under the jurisdiction of the UK, such as UK Embassies, military bases and detention facilities.

1.23 Under the provisions of section 76A of the 2000 Act, as inserted by the Crime (International Co-Operation) Act 2003, foreign surveillance teams may operate in the UK subject to certain conditions. See Chapter 5 (*Authorisation* procedures for directed surveillance) for detail.

Chapter 2

DIRECTED AND INTRUSIVE SURVEILLANCE DEFINITIONS

2.1 This chapter provides further guidance on whether covert surveillance activity is directed surveillance or intrusive surveillance, or whether an *authorisation* for either activity would not be deemed necessary.

Directed surveillance

2.2 Surveillance is directed surveillance if the following are all true:

- it is covert, but not intrusive surveillance;
- it is conducted for the purposes of a specific investigation or operation;
- it is likely to result in the obtaining of *private information* about a person (whether or not one specifically identified for the purposes of the investigation or operation);
- it is conducted otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an *authorisation* under Part II of the 2000 Act to be sought.

2.3 Thus, the planned covert surveillance of a specific person, where not intrusive, would constitute directed surveillance if such surveillance is likely to result in the obtaining of *private information* about that, or any other person.

Private information

2.4 The 2000 Act states that *private information* includes any information relating to a person's private or family life.⁷ *Private information* should be taken generally to include any aspect of a person's private or personal relationship with others, including family⁸ and professional or business relationships.

2.5 Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of *private information*. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a *public authority* of that person's activities for future consideration or analysis.⁹

Example: Two people holding a conversation on the street or in a bus may have a reasonable expectation of privacy over the contents of that conversation, even though they are associating in public. The contents of such a conversation should therefore still be considered as private information. A directed surveillance authorisation would therefore be appropriate for a public authority to record or listen to the conversation as part of a specific investigation or operation.

2.6 Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of behaviour, or if one or more pieces of information (whether or not available in the public domain) are covertly (or in some cases overtly) obtained for the purpose of making a permanent record about a person or for subsequent data processing to generate further information. In such circumstances,

⁷ See section 26(10) of the 2000 Act.

⁸ Family should be treated as extending beyond the formal relationships created by marriage or civil partnership.

⁹ Note also that a person in police custody will have certain expectations of privacy.

the totality of information gleaned may constitute *private information* even if individual records do not. Where such conduct includes covert surveillance, a directed surveillance *authorisation* may be considered appropriate.

Example: Officers of a local authority wish to drive past a café for the purposes of obtaining a photograph of the exterior. Reconnaissance of this nature is not likely to require a directed surveillance authorisation as no private information about any person is likely to be obtained or recorded. However, if the authority wished to conduct a similar exercise, for example to establish a pattern of occupancy of the premises by any person, the accumulation of information is likely to result in the obtaining of private information about that person and a directed surveillance authorisation should be considered.

2.7 *Private information* may include personal data, such as names, telephone numbers and address details. Where such information is acquired by means of covert surveillance of a person having a reasonable expectation of privacy, a directed surveillance *authorisation* is appropriate.¹⁰

Example: A surveillance officer intends to record a specific person providing their name and telephone number to a shop assistant, in order to confirm their identity, as part of a criminal investigation. Although the person has disclosed these details in a public place, there is nevertheless a reasonable expectation that the details are not being recorded separately for another purpose. A directed surveillance authorisation should therefore be sought.

¹⁰ The fact that a directed surveillance *authorisation* is available does not mean it is required. There may be other lawful means of obtaining personal data which do not involve directed surveillance.

Specific situations requiring directed surveillance authorisations

2.8 The following specific situations may also constitute directed surveillance according to the 2000 Act:

- The use of surveillance devices designed or adapted for the purpose of providing information regarding the location of a vehicle alone does not necessarily constitute directed surveillance as they do not necessarily provide *private information* about any individual but sometimes only supply information about the location of that particular device at any one time. However, the use of that information, when coupled with other surveillance activity which may obtain *private information*, could interfere with Article 8 rights. A directed surveillance *authorisation* may therefore be appropriate.¹¹
- Surveillance consisting of the interception of a communication in the course of its transmission by means of a public postal service or telecommunication system where the communication is one sent or intended for a person who has consented to the interception of communications sent by or to them and where there is no interception *warrant*¹² authorising the interception.¹³

Recording of telephone conversations

2.9 Subject to paragraph 2.8 above, the interception of communications sent by public post or by means of public telecommunications systems or private telecommunications is governed by Part I of the 2000 Act. Nothing in this code should be taken as granting dispensation from the requirements of that Part of the 2000 Act.

11 The use of such devices is also likely to require an *authorisation* for property interference under the 1994 or 1997 Act. See Chapter 7.

12 i.e. under Part 1 Chapter 1 of the 2000 Act.

13 See section 48(4) of the 2000 Act. The availability of a directed surveillance *authorisation* nevertheless does not preclude authorities from seeking an interception *warrant* under Part I of the 2000 Act in these circumstances.

2.10 The recording or monitoring of one or both ends of a telephone conversation by a surveillance device as part of an authorised directed (or intrusive) surveillance operation will not constitute interception under Part I of the 2000 Act provided the process by which the product is obtained does not involve any modification of, or interference with, the telecommunications system or its operation. This will not constitute interception as sound waves obtained from the air are not in the course of transmission by means of a telecommunications system (which, in the case of a telephone conversation, should be taken to begin with the microphone and end with the speaker). Any such product can be treated as having been lawfully obtained.

Example: A property interference authorisation may be used to authorise the installation in a private car of an eavesdropping device with a microphone, together with an intrusive surveillance authorisation to record or monitor speech within that car. If one or both ends of a telephone conversation held in that car are recorded during the course of the operation, this will not constitute unlawful interception provided the device obtains the product from the sound waves in the vehicle and not by interference with, or modification of, any part of the telecommunications system.

Intrusive surveillance

2.11 Intrusive surveillance is covert surveillance that is carried out in relation to anything taking place on residential premises or in any private vehicle, and that involves the presence of an individual on the premises or in the vehicle or is carried out by a means of a surveillance device.

2.12 The definition of surveillance as intrusive relates to the location of the surveillance, and not any other consideration of the nature of the information that is expected to be obtained. In addition, directed surveillance under the ambit of the 2010 Order is to be treated as

intrusive surveillance. Accordingly, it is not necessary to consider whether or not intrusive surveillance is likely to result in the obtaining of *private information*.

Residential premises

2.13 For the purposes of the 2000 Act, residential premises are considered to be so much of any premises as is for the time being occupied or used by any person, however temporarily, for residential purposes or otherwise as living accommodation. This specifically includes hotel or prison accommodation that is so occupied or used.¹⁴ However, common areas (such as hotel dining areas) to which a person has access in connection with their use or occupation of accommodation are specifically excluded.¹⁵

2.14 The 2000 Act further states that the concept of premises should be taken to include any place whatsoever, including any vehicle or moveable structure, whether or not occupied as land.

2.15 Examples of residential premises would therefore include:

- a rented flat currently occupied for residential purposes;
- a prison cell (or police cell serving as temporary prison accommodation);
- a hotel bedroom or suite.

2.16 Examples of premises which would not be regarded as residential would include:

- a communal stairway in a block of flats (unless known to be used as a temporary place of abode by, for example, a homeless person);
- a police cell (unless serving as temporary prison accommodation);
- a prison canteen or police interview room;
- a hotel reception area or dining room;
- the front garden or driveway of premises readily visible to the public;

¹⁴ See section 48(1) of the 2000 Act.

¹⁵ See section 48(7) of the 2000 Act.

- residential premises occupied by a *public authority* for non-residential purposes; for example, trading standards ‘house of horrors’ situations or undercover operational premises.

Private vehicles

2.17 A private vehicle is defined in the 2000 Act as any vehicle, including vessels, aircraft or hovercraft, which is used primarily for the private purposes of the person who owns it or a person otherwise having the right to use it. This would include, for example, a company car, owned by a leasing company and used for business and pleasure by the employee of a company.¹⁶

Places for legal consultation

2.18 The 2010 Order provides that directed surveillance that is carried out in relation to anything taking place on so much of any premises specified in Article 3(2) of the Order as is, at any time during the surveillance, used for the purpose of legal consultations shall be treated for the purposes of Part II of the 2000 Act as intrusive surveillance. The premises identified in Article 3(2) are:

- (a) any place in which persons who are serving sentences of imprisonment or detention, remanded in custody or committed in custody for trial or sentence may be detained;
- (b) any place in which persons may be detained under paragraph 16(1), (1A) or (2) of Schedule 2 or paragraph 2(2) or (3) of Schedule 3 to the Immigration Act 1971 or section 36(1) of the UK Border Act 2007;
- (c) police stations;
- (d) hospitals where high security psychiatric services are provided;
- (e) the place of business of any professional legal adviser; and
- (f) any place used for the sittings and business of any court, tribunal, inquest or inquiry.

¹⁶ See section 48(1) and 48 (7) of the 2000 Act.

Further considerations

2.19 Intrusive surveillance (or directed surveillance being treated as intrusive surveillance under the 2010 Order) may take place by means of a person or device located in residential premises or a private vehicle or by means of a device placed outside the premises or vehicle which consistently provides information of the same quality and detail as might be expected to be obtained from a device inside.¹⁷

Example: An observation post outside residential premises which provides a limited view compared to that which would be achievable from within the premises does not constitute intrusive surveillance. However, the use of a zoom lens, for example, which consistently achieves imagery of the same quality as that which would be visible from within the premises, would constitute intrusive surveillance.

2.20 The use of a device for the purpose of providing information about the location of any private vehicle is not considered to be intrusive surveillance.¹⁸ Such use may, however, be authorised as directed surveillance, where the recording or use of the information would amount to the covert monitoring of the movements of the occupant(s) of that vehicle. A property interference *authorisation* may be appropriate for the covert installation or deployment of the device.

Where authorisation is not required

2.21 Some surveillance activity does not constitute intrusive or directed surveillance for the purposes of Part II of the 2000 Act and no directed or intrusive surveillance *authorisation* can be provided for such activity. Such activity includes:

- covert surveillance by way of an immediate response to events;
- covert surveillance as part of general observation activities;
- covert surveillance not relating to specified grounds;

¹⁷ See section 26(5) of the 2000 Act.

¹⁸ See section 26(4) of the 2000 Act.

- overt use of CCTV and ANPR systems;¹⁹
- certain other specific situations.

2.22 Each situation is detailed and illustrated below.

Immediate response

2.23 Covert surveillance that is likely to reveal *private information* about a person but is carried out by way of an immediate response to events such that it is not reasonably practicable to obtain an *authorisation* under the 2000 Act, would not require a directed surveillance *authorisation*. The 2000 Act is not intended to prevent law enforcement *officers* fulfilling their legislative functions. To this end section 26(2)(c) of the 2000 Act provides that surveillance is not directed surveillance when it is carried out by way of an immediate response to events or circumstances the nature of which is such that it is not reasonably practicable for an *authorisation* to be sought for the carrying out of the surveillance.

Example: An authorisation under the 2000 Act would not be appropriate where police officers conceal themselves to observe suspicious persons that they come across in the course of a routine patrol.

General observation activities

2.24 The general observation duties of many law enforcement *officers* and other *public authorities* do not require *authorisation* under the 2000 Act, whether covert or overt. Such general observation duties frequently form part of the legislative functions of *public authorities*, as opposed to the pre-planned surveillance of a specific person or group of people.

¹⁹ See the Surveillance Camera Code of Practice issued under Part 2 of the Protection of Freedoms Act 2012 for guidance on the overt use of surveillance cameras, including CCTV and ANPR in public places. This applies in England and Wales.

Example 1: Plain clothes police officers on patrol to monitor a high street crime hot-spot or prevent and detect shoplifting would not require a directed surveillance authorisation. Their objective is merely to observe a location and, through reactive policing, to identify and arrest offenders committing crime. The activity may be part of a specific investigation but is general observational activity, rather than surveillance of individuals, and the obtaining of private information is unlikely. A directed surveillance authorisation need not be sought.

Example 2: Local authority officers attend a car boot sale where it is suspected that counterfeit goods are being sold, but they are not carrying out surveillance of particular individuals and their intention is, through reactive policing, to identify and tackle offenders. Again this is part of the general duties of public authorities and the obtaining of private information is unlikely. A directed surveillance authorisation need not be sought.

Example 3: Intelligence suggests that a local shopkeeper is openly selling alcohol to underage customers, without any questions being asked. A trained employee or person engaged by a public authority is deployed to act as a juvenile in order to make a purchase of alcohol. In these circumstances any relationship, if established at all, is likely to be so limited in regards to the requirements of the Act, that a public authority may conclude that a covert human intelligence source (CHIS) authorisation is unnecessary. However, if the test purchaser is wearing recording equipment and is not authorised as a CHIS, or an adult is observing, consideration should be given to granting a directed surveillance authorisation.

Example 4: Surveillance officers intend to follow and observe Z covertly as part of a pre-planned operation to determine her suspected involvement in shoplifting. It is proposed to conduct covert surveillance of Z and record her activities as part of the investigation. In this case, private life considerations are likely to arise where there is an expectation of privacy and the covert surveillance is pre-planned and not part of general observational duties or reactive policing. A directed surveillance authorisation should therefore be considered.

Surveillance not relating to specified grounds or core functions

2.25 An *authorisation* for directed or intrusive surveillance is only appropriate for the purposes of a specific investigation or operation, insofar as that investigation or operation relates to the grounds specified at section 28(3) of the 2000 Act. Covert surveillance for any other general purposes should be conducted under other legislation, if relevant, and an *authorisation* under Part II of the 2000 Act should not be sought.

2.26 The ‘core functions’ referred to by the Investigatory Powers Tribunal (*C v The Police and the Secretary of State for the Home Office – IPT/03/32/H dated 14 November 2006*) are the ‘specific public functions’, undertaken by a particular authority, in contrast to the ‘ordinary functions’ which are those undertaken by all authorities (e.g. employment issues, contractual arrangements etc.). A *public authority* may only engage the 2000 Act when in performance of its ‘core functions’. The disciplining of an employee is not a ‘core function’, although related criminal investigations may be. The protection of the 2000 Act may therefore be available in relation to associated criminal investigations so long as the activity is deemed to be necessary and proportionate.

Example 1: A police officer is suspected by his employer of undertaking additional employment in breach of discipline regulations. The police force of which he is a member wishes to conduct covert surveillance of the officer outside the police work environment. Such activity, even if it is likely to result in the obtaining of private information, does not constitute directed surveillance for the purposes of the 2000 Act as it does not relate to the discharge of the police force's core functions. It relates instead to the carrying out of ordinary functions, such as employment, which are common to all public authorities. Activities of this nature are covered by the Data Protection Act 1998 and employment practices code.

Example 2: A police officer claiming compensation for injuries allegedly sustained at work is suspected by his employer of fraudulently exaggerating the nature of those injuries. The police force of which he is a member wishes to conduct covert surveillance of the officer outside the work environment. Such activity may relate to the discharge of the police force's core functions as the police force may launch a criminal investigation. The proposed surveillance is likely to result in the obtaining of private information and, as the alleged misconduct amounts to the criminal offence of fraud, a directed surveillance authorisation may be appropriate.

CCTV and automatic number plate recognition (ANPR) cameras

2.27 The use of overt CCTV cameras by *public authorities* does not normally require an *authorisation* under the 2000 Act. Members of the public should be made aware that such systems are in use. For example, by virtue of cameras or signage being clearly visible, through the provision of information and by undertaking consultation. Guidance on their operation is provided in the

Surveillance Camera Code of Practice issued under the Protection of Freedoms Act 2012. This sets out a framework of good practice that includes existing legal obligations, including the processing of personal data under the Data Protection Act 1998 and a public authority's duty to adhere to the Human Rights Act 1998. Similarly, the overt use of ANPR systems to monitor traffic flows or detect motoring offences does not require an *authorisation* under the 2000 Act.

Example: Overt surveillance equipment, such as town centre CCTV systems or ANPR, is used to gather information as part of a reactive operation (e.g. to identify individuals who have committed criminal damage after the event). Such use does not amount to covert surveillance as the equipment was overt and not subject to any covert targeting. Use in these circumstances would not require a directed surveillance authorisation.

2.28 However, where overt CCTV or ANPR cameras are used in a covert and pre-planned manner as part of a specific investigation or operation, for the surveillance of a specific person or group of people, a directed surveillance *authorisation* should be considered. Such covert surveillance is likely to result in the obtaining of *private information* about a person (namely, a record of their movements and activities) and therefore falls properly within the definition of directed surveillance. The use of the CCTV or ANPR system in these circumstances goes beyond their intended use for the general prevention or detection of crime and protection of the public.

Example: A local police team receive information that an individual suspected of committing thefts from motor vehicles is known to be in a town centre area. A decision is taken to use the town centre CCTV system to conduct surveillance against that individual such that remains unaware that there may be any specific interest in him. This targeted, covert use of the overt town centre CCTV system to monitor and/or record that individual's movements should be considered for authorisation as directed surveillance.

Online covert activity

2.29 The use of the internet may be required to gather information prior to and/or during an operation, which may amount to directed surveillance. Whenever a public authority intends to use the internet as part of an investigation, they must first consider whether the proposed activity is likely to interfere with a person's Article 8 rights, including the effect of any collateral intrusion. Any activity likely to interfere with an individual's Article 8 rights should only be used when necessary and proportionate to meet the objectives of a specific case. Where it is considered that private information is likely to be obtained, an authorisation (combined or separate) must be sought as set out elsewhere in this code. Where an investigator may need to communicate covertly online, for example, contacting individuals using social media websites, a CHIS authorisation should be considered.

Specific situations not requiring authorisation

2.30 The following specific activities also constitute neither directed nor intrusive surveillance:

- the use of a recording device by a covert human intelligence source in respect of whom an appropriate use or conduct *authorisation* has been granted permitting them to record any information obtained in their presence;²⁰

²⁰ See section 48(3) of the 2000 Act.

- the recording, whether overt or covert, of an interview with a member of the public where it is made clear that the interview is entirely voluntary and that the interviewer is a *member of a public authority*. In such circumstances, whether the recording equipment is overt or covert, the member of the public knows that they are being interviewed by a *member of a public authority* and that information gleaned through the interview has passed into the possession of the *public authority* in question;
- the covert recording of noise where: the recording is of decibels only or constitutes non-verbal noise (such as music, machinery or an alarm) or the recording of verbal content is made at a level which does not exceed that which can be heard from the street outside or adjoining property with the naked ear. In the latter circumstance the perpetrator would normally be regarded as having forfeited any claim to privacy. In either circumstance, an *authorisation* is unlikely to be required;
- the use of apparatus outside any residential or other premises exclusively for the purpose of detecting the installation or use of a television receiver within those premises. The Regulation of Investigatory Powers (British Broadcasting Corporation) Order 2001 (SI No. 1057) permits the British Broadcasting Corporation to authorise the use of apparatus for this purpose under Part II of the 2000 Act, although such use constitutes neither directed nor intrusive surveillance;²¹
- entry on or interference with property or wireless telegraphy under section 5 of the 1994 Act or Part III of the 1997 Act (such activity may be conducted in support of surveillance, but is not in itself surveillance).²²

²¹ See section 26(6) of the 2000 Act.

²² See section 48(3) of the 2000 Act.

Chapter 3

GENERAL RULES ON AUTHORISATIONS

Overview

3.1 An *authorisation* under Part II of the 2000 Act will, providing the statutory tests are met, provide a lawful basis for a *public authority* to carry out covert surveillance activity that is likely to result in the obtaining of *private information* about a person. Similarly, an *authorisation* under section 5 of the 1994 Act or Part III of the 1997 Act will provide lawful authority for *members* of the intelligence services, police, National Crime Agency (NCA) or Her Majesty's Revenue and Customs (HMRC) to enter on, or interfere with, property or wireless telegraphy.

3.2 Responsibility for granting *authorisations* varies depending on the nature of the operation and the *public authority* involved. The relevant *public authorities* and *authorising officers* are detailed in the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010.

Necessity and proportionality

3.3 The 2000 Act, 1997 Act and 1994 Act stipulate that the person granting an *authorisation* or *warrant* for directed or intrusive surveillance, or interference with property, must believe that the activities to be authorised are necessary on one or more statutory grounds.²³

²³ These statutory grounds are laid out in sections 28(3) of the 2000 Act for directed surveillance; section 32(3) of the 2000 Act for intrusive surveillance; and section 93(2) of the 1997 Act and section 5 of the 1994 Act for property interference. They are detailed in Chapters 5, 6 and 7 for directed surveillance, intrusive surveillance and interference with property respectively.

3.4 If the activities are deemed necessary on one or more of the statutory grounds, the person granting the *authorisation* or *warrant* must also believe that they are proportionate to what is sought to be achieved by carrying them out. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.

3.5 The *authorisation* will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render intrusive actions proportionate. Similarly, an offence may be so minor that any deployment of covert techniques would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

3.6 The following elements of proportionality should therefore be considered:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

3.7 It is important therefore that all those involved in undertaking directed or intrusive surveillance activities or interference with property under the 2000 Act, 1997 Act or 1994 Act are fully aware of the extent and limits of the *authorisation* or *warrant* in question.

Example: An individual is suspected of carrying out a series of criminal damage offences at a local shop, after a dispute with the owner. It is suggested that a period of directed surveillance should be conducted against him to record his movements and activities for the purposes of preventing or detecting crime. Although these are legitimate grounds on which directed surveillance may be conducted, it is unlikely that the resulting interference with privacy will be proportionate in the circumstances of the particular case. In particular, the obtaining of private information on the individual's daily routine is unlikely to be necessary or proportionate in order to investigate the activity of concern. Instead, other less intrusive means are likely to be available, such as overt observation of the location in question until such time as a crime may be committed.

Collateral intrusion

3.8 Before authorising *applications* for directed or intrusive surveillance, the *authorising officer* should also take into account the risk of obtaining *private information* about persons who are not subjects of the surveillance or property interference activity (collateral intrusion).

3.9 Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those who are not the intended subjects of the surveillance activity. Where such collateral intrusion is unavoidable, the activities may still be authorised, provided this intrusion is considered proportionate to what is sought to be achieved. The same proportionality tests apply to the likelihood of collateral intrusion as to intrusion into the privacy of the intended subject of the surveillance.

3.10 All *applications* should therefore include an assessment of the risk of collateral intrusion and details of any measures taken to limit this, to enable the *authorising officer* fully to consider the proportionality of the proposed actions.

Example: HMRC seeks to conduct directed surveillance against T on the grounds that this is necessary and proportionate for the collection of a tax. It is assessed that such surveillance will unavoidably result in the obtaining of some information about members of T's family, who are not the intended subjects of the surveillance. The authorising officer should consider the proportionality of this collateral intrusion, and whether sufficient measures are to be taken to limit it, when granting the authorisation. This may include not recording or retaining any material obtained through such collateral intrusion.

3.11 Where it is proposed to conduct surveillance activity or property interference specifically against individuals who are not suspected of direct or culpable involvement in the overall matter being investigated, interference with the privacy or property of such individuals should not be considered as collateral intrusion but rather as intended intrusion. Any such surveillance or property interference activity should be carefully considered against the necessity and proportionality criteria as described above (paragraphs 3.3–3.8).

Example: A law enforcement agency seeks to conduct a covert surveillance operation to establish the whereabouts of N in the interests of preventing a serious crime. It is proposed to conduct directed surveillance against P, who is an associate of N but who is not assessed to be involved in the crime, in order to establish the location of N. In this situation, P will be the subject of the directed surveillance authorisation and the authorising officer should consider the necessity and proportionality of conducting directed surveillance against P, bearing in mind the availability of any other less intrusive means to identify N's whereabouts. It may be the case that directed surveillance of P will also result in obtaining information about P's family, which in this instance would represent collateral intrusion also to be considered by the authorising officer.

Combined authorisations

3.12 A single *authorisation* may combine:

- any number of *authorisations* under Part II of the 2000 Act;²⁴
- an *authorisation* under Part II of the 2000 Act²⁵ and an *authorisation* under Part III of the 1997 Act;
- a *warrant* for intrusive surveillance under Part II of the 2000 Act²⁶ and a *warrant* under section 5 of the 1994 Act.

3.13 For example, a single *authorisation* may combine *authorisations* for directed and intrusive surveillance. However, the provisions applicable for each of the *authorisations* must be considered separately by the appropriate *authorising officer*. Thus, a police superintendent could authorise the directed surveillance element but the intrusive surveillance element would need the separate *authorisation* of a chief constable and the approval of a Surveillance Commissioner, unless the case is urgent.

3.14 The above considerations do not preclude *public authorities* from obtaining separate *authorisations*.

Collaborative working

3.15 Any person granting or applying for an *authorisation* will also need to be aware of particular sensitivities in the local community where the surveillance is taking place and of any similar activities being undertaken by other *public authorities* which could impact on the deployment of surveillance. It is therefore recommended that where an *authorising officer* from a *public authority* considers that conflicts might arise they should consult a senior *officer* within the police force area in which the investigation or operation is to take place.

²⁴ See section 43(2) of the 2000 Act.

²⁵ On the *application* of a *member* of a police force, NCA, a customs *officer* or an *officer* of the CMA. See section 33(5) of the 2000 Act.

²⁶ On the *application* of a *member* of the intelligence services. See section 42(2) of the 2000 Act.

3.16 In cases where one agency or force is acting on behalf of another, the tasking agency should normally obtain or provide the *authorisation* under Part II of the 2000 Act. For example, where surveillance is carried out by the police on behalf of HMRC, *authorisations* would usually be sought by HMRC and granted by the appropriate *authorising officer*. Where the operational support of other agencies (in this example, the police) is foreseen, this should be specified in the *authorisation*.

3.17 Where possible, *public authorities* should seek to avoid duplication of *authorisations* as part of a single investigation or operation. For example, where two agencies are conducting directed or intrusive surveillance as part of a joint operation, only one *authorisation* is required. Duplication of *authorisations* does not affect the lawfulness of the activities to be conducted, but may create an unnecessary administrative burden on authorities.

3.18 Where an individual or a non-governmental organisation is acting under direction of a public authority then they are acting as an agent of that public authority and any activities they conduct which meet the 2000 Act definitions of directed or intrusive surveillance or amount to property interference for the purposes of the 1994 or 1997 Act, should be considered for authorisation under those Acts.

3.19 There are three further important considerations with regard to collaborative working:

3.20 NCA and HMRC *applications* for directed or intrusive surveillance and property interference, and Competition and Markets Authority (CMA) *applications* for intrusive surveillance, must only be made by a *member* or *officer* of the same force or agency as the *authorising officer*, regardless of which force or agency is to conduct the activity.

3.21 Police *applications* for directed or intrusive surveillance and property interference must only be made by a *member* or *officer* of the same force as the *authorising officer*, unless the Chief Officers of the forces in question have made a collaboration agreement under the Police Act 1996 and the collaboration agreement permits applicants and *authorising officers* to be from different forces.

3.22 *Authorisations* for intrusive surveillance relating to residential premises, and *authorisations* for property interference, may only authorise conduct where the premises or property in question are in the area of operation of the force or agency applying for the *authorisation*. This requirement does not apply where the Chief *Officers* of two or more police forces have made a collaboration agreement under the Police Act 1996 and the collaboration agreement permits *authorising officers* to authorise conduct in relation to premises or property in the force areas of forces other than their own which are party to the agreement.

Reviewing authorisations

3.23 Regular reviews of all *authorisations* should be undertaken to assess the need for the surveillance or property interference activity to continue. The results of a review should be retained for at least three years (see Chapter 8). Particular attention is drawn to the need to review *authorisations* frequently where the surveillance or property interference involves a high level of intrusion into private life or significant collateral intrusion, or *confidential information* is likely to be obtained.

3.24 In each case the frequency of reviews should be considered at the outset by the *authorising officer* or, for those subject to *authorisation* by the *Secretary of State*, the *member* or *officer* who made the *application* within the *public authority* concerned. This should be as frequently as is considered necessary and practicable.

3.25 In some cases it may be appropriate for an *authorising officer* to delegate the responsibility for conducting any reviews to a subordinate *officer*. The *authorising officer* is, however, usually best placed to assess whether the *authorisation* should continue or whether the criteria on which he or she based the original decision to grant an *authorisation* have changed sufficiently to cause the *authorisation* to be revoked. Support staff can do the necessary research and prepare the review process but the actual review is the responsibility of the original *authorising officer* and should, as a matter of good practice, be conducted by them or, failing that, by an *officer* who would be entitled to grant a new *authorisation* in the same terms.

3.26 Any proposed or unforeseen changes to the *nature* or extent of the surveillance operation that may result in the further or greater intrusion into the private life of any person should also be brought to the attention of the *authorising officer* by means of a review. The *authorising officer* should consider whether the proposed changes are proportionate (bearing in mind any extra intended intrusion into privacy or collateral intrusion), before approving or rejecting them. Any such changes must be highlighted at the next renewal if the *authorisation* is to be renewed.

3.27 Where a directed or intrusive surveillance *authorisation* provides for the surveillance of unidentified individuals whose identity is later established, the terms of the *authorisation* should be refined at a review to include the identity of these individuals. It would be appropriate to convene such a review specifically for this purpose. This process will not require a fresh *authorisation*, providing the scope of the original *authorisation* envisaged surveillance of such individuals. Such changes must be highlighted at the next renewal if the *authorisation* is to be renewed.

Example: A directed surveillance authorisation is obtained by the police to authorise surveillance of ‘X and his associates’ for the purposes of investigating their suspected involvement in a crime. X is seen meeting with A in a café and it is assessed that subsequent surveillance of A will assist the investigation. Surveillance of A may continue (he is an associate of X) but the directed surveillance authorisation should be amended at a review to include ‘X and his associates, including A’.

General best practices

3.28 The following guidelines should be considered as best working practices by all *public authorities* with regard to all *applications* for *authorisations* covered by this code:

- *applications* should avoid any repetition of information;

- information contained in *applications* should be limited to that required by the relevant legislation;²⁷
- where *authorisations* are granted orally under urgency procedures (see Chapters 5, 6 and 7 on *authorisation* procedures), a record detailing the actions authorised and the reasons why the urgency procedures were used should be recorded by the *applicant* and *authorising officer* as a priority. There is then no requirement subsequently to submit a full written *application*;
- an *application* should not require the sanction of any person in a *public authority* other than the *authorising officer*;
- where it is foreseen that other agencies will be involved in carrying out the surveillance, these agencies should be detailed in the *application*;
- *authorisations* should not generally be sought for activities already authorised following an *application* by the same or a different *public authority*.

3.29 Furthermore, it is considered good practice that within every relevant *public authority*, a senior responsible *officer*²⁸ should be responsible for:

- the integrity of the process in place within the *public authority* to authorise directed and intrusive surveillance and interference with property or wireless telegraphy;
- compliance with Part II of the 2000 Act, Part III of the 1997 Act and with this code;
- engagement with the Commissioners and inspectors when they conduct their inspections, and
- where necessary, overseeing the implementation of any post-inspection action plans recommended or approved by a Commissioner.

²⁷ As laid out in Chapters 5, 6 and 7 of this code.

²⁸ The senior responsible *officer* should be a person holding the office, rank or position of an *authorising officer* within the relevant *public authority*.

Local authorities

3.30 The Protection of Freedoms Act 2012 amended the 2000 Act to make local authority authorisations subject to judicial approval. The change means that local authorities need to obtain an order approving the grant or renewal of an authorisation from a judicial authority, before it can take effect. In England and Wales an application for such an Order must be made to a Justice of the Peace (JP). If the JP is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate, he or she will issue an order approving the grant or renewal for the use of the technique as described in the application. The amendment means that local authorities are no longer able to orally authorise the use of RIPA techniques. All authorisations must be made in writing and require JP approval. The authorisation cannot commence until this has been obtained.

3.31 In Scotland this requirement only applies to authorisations for communications data as the use of the other techniques is governed by RIP(S)A. Where such an authorisation is required by a local authority in Scotland, an application for grant or renewal should be made to a sheriff. For other activities/authorisations, local authorities in Scotland should refer to devolved legislation. In Northern Ireland this requirement only applies to authorisations where the grant or renewal relates to a Northern Ireland excepted or reserved matter. Where such an authorisation is required by a local authority in Northern Ireland, an application for a grant or renewal should be made to a district judge. For other authorisations, local authorities in Northern Ireland should refer to the general requirements for authorisation set out in this code.

3.32 The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 has the following effects:

- Local authorities in England and Wales can only authorise use of directed surveillance under RIPA to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least six months'

imprisonment **or** are related to the underage sale of alcohol and tobacco. The offences relating to the latter are in Article 7A of the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010.

- Local authorities **cannot** authorise directed surveillance for the purpose of preventing disorder unless this involves a criminal offence(s) punishable (whether on summary conviction or indictment) by a maximum term of at least six months' imprisonment.
- Local authorities may therefore continue to authorise use of directed surveillance in more serious cases as long as the other tests are met – i.e. that it is necessary and proportionate and where prior approval from a JP has been granted. Examples of cases where the offence being investigated attracts a maximum custodial sentence of six months or more could include more serious criminal damage, dangerous waste dumping and serious or serial benefit fraud.
- Local authorities may also continue to authorise the use of directed surveillance for the purpose of preventing or detecting specified criminal offences relating to the underage sale of alcohol and tobacco where the necessity and proportionality test is met and prior approval from a JP has been granted.
- A local authority **may not authorise** the use of directed surveillance under RIPA to investigate disorder that does not involve criminal offences or to investigate low-level offences which may include, for example, littering, dog control and fly-posting.

3.33 The provisions of the Order, detailed above, do not apply to Scotland and Northern Ireland.

3.34 Within local authorities, the senior responsible officer should be a member of the corporate leadership team and should be responsible for ensuring that all *authorising officers* are of an appropriate standard in light of any recommendations in the inspection reports prepared by the Office of the Surveillance Commissioner. Where an inspection report highlights concerns about the standards of *authorising officers*, this individual will be responsible for ensuring the concerns are addressed.

3.35 Elected members of a local authority should review the authority's use of the 2000 Act and set the policy at least once a year. They should also consider internal reports on use of the 2000 Act on a regular basis to ensure that it is being used consistently with the local authority's policy and that the policy remains fit for purpose.

Chapter 4

LEGALLY PRIVILEGED AND CONFIDENTIAL INFORMATION

Overview

4.1 The 2000 Act does not provide any special protection for ‘*confidential information*’, although the 1997 Act makes special provision for certain categories of *confidential information*. Nevertheless, particular care should be taken in cases where the subject of the investigation or operation might reasonably expect a high degree of privacy, or where *confidential information* is involved. *Confidential information* consists of communications subject to *legal privilege*, communications between a *Member of Parliament* and another person on constituency matters, confidential personal information, or confidential journalistic material. So, for example, extra care should be taken where, by undertaking surveillance of an individual it is likely that knowledge will be acquired of communications between a minister of religion and that individual relating to the latter’s spiritual welfare, or between a *Member of Parliament* and that individual where he or she is a constituent relating to constituency matters, or wherever matters of medical or journalistic confidentiality or *legal privilege* may be involved.

4.2 *Authorisations* under the 1997 Act likely to result in the acquisition of knowledge of matters subject to *legal privilege*, confidential personal information or confidential journalistic material require (other than in urgent cases) the approval of a Surveillance Commissioner.

4.3 *Authorisations* for directed surveillance of legal consultations falling within the 2010 Order, must comply with the enhanced *authorisation* regime described below. In cases where it is likely that knowledge of *confidential information* will be acquired, the use of covert

surveillance is subject to a higher level of *authorisation* e.g. a Chief *Officer*. Annex A lists the *authorising officer* for each *public authority* permitted to authorise such surveillance.

Material subject to legal privilege: introduction

4.4 Covert surveillance likely or intended to result in the acquisition of knowledge of matters subject to *legal privilege* may take place in circumstances covered by the 2010 Order or in other circumstances. Similarly, property interference may be necessary in order to effect surveillance described in the same Order, or in other circumstances where knowledge of matters subject to *legal privilege* is likely to be obtained.

4.5 The 2010 Order, provides that directed surveillance that is carried out in relation to anything taking place on so much of any premises specified in Article 3(2) of the Order as is, at any time during the surveillance, used for the purposes of ‘legal consultations’ shall be treated for the purposes of Part II of the 2000 Act as intrusive surveillance.

4.6 The Order defines ‘legal consultation’ for these purposes. It means:

- (a) a consultation between a professional legal adviser and his client or any person representing his client, or
- (b) a consultation between a professional legal adviser or his client or any such representative and a medical practitioner made in connection with or in contemplation of legal proceedings and for the purposes of such proceedings.

4.7 The definition of ‘legal consultation’ in the 2010 Order, does not distinguish between legal consultations which are legally privileged, wholly or in part, and legal consultations which may be in furtherance of a criminal purpose are therefore not protected by *legal privilege*. Covert surveillance of all legal consultations covered by the 2010 Order (whether protected by *legal privilege* or not) is to be treated as intrusive surveillance.

4.8 *'Legal privilege'* is defined in section 98 of the 1997 Act. This definition should be used to determine how to handle material obtained through surveillance authorised under RIPA, including through surveillance which is treated as intrusive surveillance as a result of the 2010 Order. As discussed below, special safeguards apply to matters subject to *legal privilege*.

4.9 Under the definition in the 1997 Act, *legal privilege* does not apply to communications or items held, or oral communications made, with the intention of furthering a criminal purpose (whether the lawyer is acting unwittingly or culpably). Legally privileged communications or items will lose their protection for these other purposes if the professional legal adviser intends to hold or use them for a criminal purpose. But privilege is not lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence.

Tests to be applied when authorising or approving covert surveillance or property interference likely or intended to result in the acquisition of knowledge of matters subject to legal privilege

4.10 All *applications* for covert surveillance or property interference that may result in the acquisition of knowledge of matters subject to *legal privilege* should state whether the covert surveillance or property interference is intended to obtain knowledge of matters subject to *legal privilege* as defined by section 98 of the 1997 Act.

4.11 If the covert surveillance or property interference is not intended to result in the acquisition of knowledge of matters subject to *legal privilege*, but it is likely that such knowledge will nevertheless be acquired during the operation, the *application* should identify all steps which will be taken to mitigate the risk of acquiring it. If the risk cannot be removed entirely, the *application* should explain what steps will be taken to ensure that any knowledge of matters subject to *legal privilege* which is obtained is not used in law enforcement investigations or criminal prosecutions.

4.12 Where covert surveillance or property interference is likely or intended to result in the acquisition of knowledge of matters subject to *legal privilege*, an *authorisation* shall only be granted or approved if the *authorising officer*, *Secretary of State* or approving Surveillance Commissioner, as appropriate, is satisfied that there are exceptional and compelling circumstances that make the *authorisation* necessary:

- Where the surveillance or property interference is not intended to result in the acquisition of knowledge of matters subject to *legal privilege*, such exceptional and compelling circumstances may arise in the interests of national security or the economic well-being of the UK, or for the purpose of preventing or detecting serious crime;
- Where the surveillance or property interference is intended to result in the acquisition of knowledge of matters subject to *legal privilege*, such circumstances will arise only in a very restricted range of cases, such as where there is a threat to life or limb, or to national security, and the surveillance or property interference is reasonably regarded as likely to yield intelligence necessary to counter the threat.

4.13 Further, in considering any *authorisation* for covert surveillance or property interference likely or intended to result in the acquisition of knowledge of matters subject to *legal privilege*, the *authorising officer*, *Secretary of State* or approving Surveillance Commissioner, as appropriate, must be satisfied that the proposed covert surveillance or property interference is proportionate to what is sought to be achieved. In relation to intrusive surveillance, including surveillance to be treated as intrusive as a result of the 2010 Order, section 32(4) will apply.

4.14 Directed surveillance likely to result in the acquisition of knowledge of matters subject to *legal privilege* may be authorised only by *authorising officers* entitled to grant *authorisations* in respect of *confidential information*. Intrusive surveillance, including surveillance which is treated as intrusive by virtue of the 2010 Order, or property interference likely to result in the acquisition of material subject to *legal privilege* may only be authorised by *authorising officers* entitled to grant intrusive surveillance or property interference *authorisations*.

4.15 Property interference likely to result in the acquisition of such material is subject to prior approval by a Surveillance Commissioner (unless the *Secretary of State* is the relevant *authorising officer* or the case is urgent). Intrusive surveillance, including surveillance which is treated as intrusive by virtue of the 2010 Order is subject to prior approval by a Surveillance Commissioner (unless the *Secretary of State* is the relevant *authorising officer* or the case is urgent).

Surveillance under the Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010

4.16 As noted above, the 2010 Order provides that directed surveillance that is carried out in relation to anything taking place on so much of any premises specified in Article 3(2) of the Order as is, at any time during the surveillance, used for the purposes of ‘legal consultations’ shall be treated for the purposes of Part II of the 2000 Act as intrusive surveillance.

4.17 As a result of the 2010 Order, such surveillance cannot be undertaken without the prior approval of a Surveillance Commissioner (with the exception of urgent *authorisations* or *authorisations* granted by the *Secretary of State*).

4.18 The locations specified in the Order are:

- (a) any place in which persons who are serving sentences of imprisonment or detention, remanded in custody or committed in custody for trial or sentence may be detained;
- (b) any place in which persons may be detained under paragraph 16(1), (1A) or (2) of Schedule 2 or paragraph 2(2) or (3) of Schedule 3 to the Immigration Act 1971 or section 36(1) of the UK Border Act 2007;
- (c) any place in which persons may be detained under Part VI of the Criminal Procedure (Scotland) Act 1995, the Mental Health (Care and Treatment) (Scotland) Act 2003 or the Mental Health Act 2003;
- (d) police stations;

- (e) the place of business of any professional legal adviser;
- (f) any place used for the sittings and business of any court, tribunal, inquest or inquiry.

4.19 With the exception of urgent *applications* and *authorisations* granted by the *Secretary of State*, *authorisations* for surveillance which is to be treated as intrusive surveillance as a result of the 2010 Order shall not take effect until such time as:

- (a) the *authorisation* has been approved by a Surveillance Commissioner; and
- (b) written notice of the Commissioner's decision to approve the *authorisation* has been given to the *authorising officer*.

4.20 If an *authorisation* is to be granted by the *Secretary of State*, the provisions in Chapter 6 apply.

Property interference under the 1997 Act likely to result in the acquisition of knowledge of matters subject to legal privilege

4.21 With the exception of urgent *authorisations*, where it is believed that the action authorised is likely to result in the acquisition of knowledge of matters subject to *legal privilege* an *authorisation* under the 1997 Act shall not take effect until such time as:

- (a) the *authorisation* has been approved by a Surveillance Commissioner; and
- (b) written notice of the Commissioner's decision to approve the *authorisation* has been given to the *authorising officer*.

The use and handling of matters subject to legal privilege

4.22 Matters subject to legally privilege are particularly sensitive and surveillance which acquires such material may give rise to issues under Article 6 of the ECHR (right to a fair trial) as well as engaging Article 8.

4.23 Where public authorities deliberately acquire knowledge of matters subject to *legal privilege*, they may use that knowledge to counter the threat which led them to acquire it, but it will not be admissible in court. Public authorities should ensure that knowledge of matters subject to *legal privilege*, whether or not it is acquired deliberately, is kept separate from law enforcement investigations or criminal prosecutions.

4.24 In cases likely to result in the acquisition of knowledge of matters subject to *legal privilege*, the *authorising officer* or Surveillance Commissioner may require regular reporting so as to be able to decide whether the *authorisation* should continue. In those cases where legally privileged material has been acquired and retained, the matter should be reported to the *authorising officer* by means of a review and to the relevant Commissioner or Inspector during his next inspection (at which the material should be made available if requested).

4.25 A substantial proportion of the communications between a lawyer and his or her client(s) may be subject to *legal privilege*. Therefore, in any case where a lawyer is the subject of an investigation or operation, *authorising officers* should consider whether the special safeguards outlined in this chapter apply. Any material which has been retained from any such investigation or operation should be notified to the relevant Commissioner or Inspector during his or her next inspection and made available on request.

4.26 Where there is any doubt as to the handling and dissemination of knowledge of matters which may be subject to *legal privilege*, advice should be sought from a legal adviser within the relevant *public authority* before any further dissemination of the information takes place. Similar advice should also be sought where there is doubt over whether information is not subject to *legal privilege* due to the ‘in furtherance of a criminal purpose’ exception. The retention of legally privileged material, or its dissemination to an outside body, should be accompanied by a clear warning that it is subject to *legal privilege*. It should be safeguarded by taking reasonable steps to ensure there is no possibility of it becoming available, or its contents becoming known, to any person whose possession of it might prejudice any criminal or civil proceedings to which the information relates. Any

dissemination of legally privileged material to an outside body should be notified to the relevant Commissioner or Inspector during his or her next inspection.

Confidential information

4.27 Special consideration must also be given to *authorisations* that involve confidential personal information, confidential constituent information and confidential journalistic material. Where such material has been acquired and retained, the matter should be reported to the relevant Commissioner or Inspector during his or her next inspection and the material be made available if requested.

4.28 Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling of a person (whether living or dead) who can be identified from it.²⁹ Such information, which can include both oral and written communications, is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. Examples include consultations between a health professional and a patient, or information from a patient's medical records.

4.29 Confidential constituent information is information relating to communications between a *Member of Parliament* and a constituent in respect of constituency matters. Again, such information is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation.

4.30 Confidential journalistic material includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking.

²⁹ **Spiritual counselling** means conversations between a person and a religious authority acting in an official capacity, where the individual being counselled is seeking or the religious authority is imparting forgiveness, absolution or the resolution of conscience in accordance with their faith.

4.31 Where there is any doubt as to the handling and dissemination of *confidential information*, advice should be sought from a legal adviser within the relevant *public authority* before any further dissemination of the material takes place.

Chapter 5

AUTHORISATION PROCEDURES FOR DIRECTED SURVEILLANCE

Authorisation criteria

5.1 Under section 28(3) of the 2000 Act an *authorisation* for directed surveillance may be granted by an *authorising officer* where he or she believes that the *authorisation* is necessary in the circumstances of the particular case on the grounds that it is:

- (a) in the interests of national security;^{30,31}
- (b) for the purpose of preventing or detecting³² crime or of preventing disorder;
- (c) in the interests of the economic well-being of the UK;
- (d) in the interests of public safety;
- (e) for the purpose of protecting public health;³³

30 One of the functions of the Security Service is the protection of national security and in particular the protection against threats from terrorism. An *authorising officer* in another *public authority* shall not issue a directed surveillance *authorisation* under Part II of the 2000 Act where the investigation or operation falls within the responsibilities of the Security Service, as set out above, except where the investigation or operation is to be carried out by a Special Branch or other police unit with formal counter-terrorism responsibilities (such as Counter Terrorism Units, Counter Terrorism Intelligence Units and Counter Terrorism Command) or where the Security Service has agreed that another *public authority* can carry out a directed surveillance investigation or operation which would fall within the responsibilities of the Security Service.

31 HM Forces may also undertake operations in connection with a military threat to national security and other operations in connection with national security in support of the Security Service, the Police Service of Northern Ireland or other Civil Powers.

32 Detecting crime is defined in section 81(5) of the 2000 Act and is applied to the 1997 Act by section 134 of that Act (as amended). Preventing or detecting crime goes beyond the prosecution of offenders and includes actions taken to avert, end or disrupt the commission of criminal offences.

33 This could include investigations into infectious diseases, contaminated products or the illicit sale of pharmaceuticals.

- (f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;³⁴ or
- (g) for any other purpose prescribed by an order made by the *Secretary of State*.³⁵

5.2 The *authorising officer* must also believe that the surveillance is proportionate to what it seeks to achieve (see 3.3–3.12).

Relevant public authorities

5.3 The *public authorities* entitled to authorise directed surveillance (including to acquire *confidential information*, with specified higher *authorisation*), are listed in Schedule 1 to the 2000 Act. The specific purposes for which each *public authority* may obtain a directed surveillance *authorisation* are laid out in the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010.

Authorisation procedures

5.4 Responsibility for authorising the carrying out of directed surveillance rests with the *authorising officer* and requires the personal authority of the *authorising officer*. The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 designates the *authorising officer* for each different *public authority* and the *officers* entitled to act in urgent cases. Where an *authorisation* for directed surveillance is combined with a *Secretary of State authorisation* for intrusive surveillance, the combined *authorisation* must be issued by the *Secretary of State*.

5.5 An *authorising officer* must give *authorisations* in writing, except that in urgent cases they may be given orally by the *authorising officer* or in writing by the *officer* entitled to act in urgent cases. In such cases, a record that the *authorising officer* has expressly authorised the action

³⁴ This could only be for a purpose which satisfies the criteria set out in Article 8(2) of the ECHR.

³⁵ This could only be for a purpose which satisfies the criteria set out in Article 8(2) of the ECHR.

should be recorded in writing by both the *authorising officer* and the applicant as soon as is reasonably practicable, together with the information detailed below.

5.6 A case is not normally to be regarded as urgent unless the time that would elapse before the *authorising officer* was available to grant the *authorisation* would, in the judgement of the person giving the *authorisation*, be likely to endanger life or jeopardise the investigation or operation for which the *authorisation* was being given. An *authorisation* is not to be regarded as urgent where the need for an *authorisation* has been neglected or the urgency is of the *authorising officer's* or *applicant's* own making.

5.7 *Authorising officers* should not normally be responsible for authorising operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable, especially in the case of small organisations, or where it is necessary to act urgently or for security reasons. Where an *authorising officer* authorises such an investigation or operation the centrally retrievable record of *authorisations* (see Chapter 8) should highlight this and the attention of a Commissioner or Inspector should be invited to it during his or her next inspection.

Information to be provided in applications for authorisation

5.8 A written *application* for a directed surveillance *authorisation* should describe any conduct to be authorised and the purpose of the investigation or operation. The *application* should also include:

- the reasons why the *authorisation* is necessary in the particular case and on the grounds (e.g. for the purpose of preventing or detecting crime) listed in section 28(3) of the 2000 Act;
- the nature of the surveillance;
- the identities, where known, of those to be the subject of the surveillance;
- a summary of the intelligence case and appropriate unique intelligence references where applicable;

- an explanation of the information which it is desired to obtain as a result of the surveillance;
- the details of any potential collateral intrusion and why the intrusion is justified;
- the details of any *confidential information* that is likely to be obtained as a consequence of the surveillance;
- the reasons why the surveillance is considered proportionate to what it seeks to achieve;
- the level of authority required (or recommended where that is different) for the surveillance; and,
- a subsequent record of whether *authorisation* was given or refused, by whom, and the time and date this happened.

5.9 In urgent cases, the above information may be supplied orally. In such cases the *authorising officer* and applicant, where applicable, should also record the following information in writing, as soon as is reasonably practicable (it is not necessary to record further detail):

- the identities of those subject to surveillance;
- the nature of the surveillance as defined at 1.9;
- the reasons why the *authorising officer* considered the case so urgent that an oral instead of a written *authorisation* was given; and,
- where the *officer* entitled to act in urgent cases has given written authority, the reasons why it was not reasonably practicable for the *application* to be considered by the *authorising officer* should also be recorded.

Duration of authorisations

5.10 A written *authorisation* granted by an *authorising officer* will cease to have effect (unless renewed or cancelled) at the end of a period of three months beginning with the day when the authorisation was granted.

5.11 Urgent oral *authorisations* or written *authorisations* granted by a person who is entitled to act only in urgent cases will, unless renewed, cease to have effect after 72 hours, beginning with the time when the *authorisation* was granted.

Renewals

5.12 If, at any time before an *authorisation* for directed surveillance granted by a *member* of the intelligence services would cease to have effect, a *member* of the intelligence services who is entitled to grant such *authorisations* considers that it is necessary for the *authorisation* to continue on the grounds of national security or in the interests of the economic well-being of the UK, he or she may renew it for a further period of six months, beginning with the day on which it would have ceased to have effect but for the renewal.

5.13 If, at any time before any other directed surveillance *authorisation* would cease to have effect, the *authorising officer* considers it necessary for the *authorisation* to continue for the purpose for which it was given, he or she may renew it in writing for a further period of three months. Renewals may also be granted orally in urgent cases and last for a period of 72 hours. The renewal will take effect at the time at which the *authorisation* would have ceased to have effect but for the renewal.

5.14 An *application* for renewal should not be made until shortly before the *authorisation* period is drawing to an end. Any person who would be entitled to grant a new *authorisation* can renew an *authorisation*.

5.15 All *applications* for the renewal of a directed surveillance *authorisation* should record (at the time of *application*, or when reasonably practicable in the case of urgent cases approved orally):

- whether this is the first renewal or every occasion on which the *authorisation* has been renewed previously;
- any significant changes to the information in the initial *application*;
- the reasons why the *authorisation* for directed surveillance should continue;
- the content and value to the investigation or operation of the information so far obtained by the surveillance;
- the results of regular reviews of the investigation or operation.

5.16 *Authorisations* may be renewed more than once, if necessary and provided they continue to meet the criteria for *authorisation*. The details of any renewal should be centrally recorded (see Chapter 8).

Cancellations

5.17 During a review, the *authorising officer* who granted or last renewed the *authorisation* may amend specific aspects of the *authorisation*, for example, to cease surveillance against one of a number of named subjects or to discontinue the use of a particular tactic. They must cancel the *authorisation* if satisfied that the directed surveillance as a whole no longer meets the criteria upon which it was authorised. Where the original *authorising officer* is no longer available, this duty will fall on the person who has taken over the role of *authorising officer* or the person who is acting as *authorising officer* (see the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010).

5.18 As soon as the decision is taken that directed surveillance should be discontinued, the instruction must be given to those involved to stop all surveillance of the subject(s). The date the *authorisation* was cancelled should be centrally recorded and documentation of any instruction to cease surveillance should be retained (see Chapter 8). There is no requirement for any further details to be recorded when cancelling a directed surveillance *authorisation*. However effective practice suggests that a record should be retained detailing the product obtained from the surveillance and whether or not objectives were achieved.

Foreign surveillance teams operating in UK

5.19 The provisions of section 76A of the 2000 Act as inserted by the Crime (International Co-Operation) Act 2003 provide for foreign surveillance teams to operate in the UK, subject to the following procedures and conditions.

5.20 Where a foreign police or customs officer, who is conducting directed or intrusive surveillance activity outside the UK, needs to enter the UK for the purposes of continuing that surveillance, and

where it is not reasonably practicable for a UK officer to carry out the surveillance under the authorisation of Part II of the 2000 Act (or of RIP(S)A), the foreign officer must notify a person designated by the Director General of NCA immediately after entry to the UK and shall request (if this has not been done already) that an application for authorisation of such surveillance be made under Part II of the 2000 Act (or RIP(S)A 2000).

5.21 The foreign officer may then continue to conduct surveillance for a period of five hours beginning with the time when the officer enters the UK. The foreign officer may only carry out the surveillance, however, in places to which members of the public have or are permitted to have access, whether on payment or otherwise. The surveillance authorisation, if obtained, will then authorise the foreign officers to conduct such surveillance beyond the five-hour period in accordance with the general provisions of the 2000 Act.

Chapter 6

AUTHORISATION PROCEDURES FOR INTRUSIVE SURVEILLANCE

General authorisation criteria

6.1 An *authorisation* for intrusive surveillance may be granted by the *Secretary of State* – for *applications* by the intelligence services, the Ministry of Defence or HM Forces³⁶ – or by a *senior authorising officer* or designated deputy of the police, NCA, HMRC or CMA, as listed in section 32(6) and 34(6) of the 2000 Act.

6.2 In many cases an operation using covert techniques may involve both directed or intrusive surveillance and property interference. This can be authorised as a combined *authorisation*, although the criteria for *authorisation* of each activity must be considered separately (see above, on combined *authorisations*).

6.3 Under section 32(2), (3) and (3A) of the 2000 Act the *Secretary of State* or the *senior authorising officer* or designated deputy may only authorise intrusive surveillance if they believe:

- (a) that the *authorisation* is necessary in the circumstances of the particular case on the grounds that it is:
 - in the interests of national security;³⁷

³⁶ Or any other *public authority* designated for this purpose under section 41(1) of the 2000 Act.

³⁷ A *senior authorising officer* or designated deputy of a law enforcement agency shall not issue an *authorisation* for intrusive surveillance where the investigation or operation is within the responsibilities of one of the intelligence services and properly falls to be authorised by *warrant* issued by the *Secretary of State* under Part II of the 2000 Act or the 1994 Act.

- for the purpose of preventing or detecting serious crime;³⁸
- in the interests of the economic well-being of the UK; or
- (in the case of the CMA) for the purpose of preventing or detecting an offence under section 188 of the Enterprise Act 2002 (cartel offence);

and

- (b) that the surveillance is proportionate to what is sought to be achieved by carrying it out.

6.4 When deciding whether an *authorisation* is necessary and proportionate, it is important to consider whether the information which it is thought necessary to obtain by means of the intrusive surveillance could reasonably be obtained by other less intrusive means.

Authorisation procedures for the police, NCA, HMRC and CMA – senior authorising officers and designated deputies

6.5 The *senior authorising officers* for these bodies are listed in section 32(6) of the 2000 Act. If the *senior authorising officer* is absent³⁹ then, under section 34(2) of the 2000 Act, an *authorisation* can be given by the designated deputy as provided for in section 12A of the Police Act 1996, section 18 of the Police and Fire Reform (Scotland) Act 2012 and section 25 of the City of London Police Act 1839.

³⁸ Serious crime is defined in section 81(2) and (3) as crime that comprises an offence for which a person who has attained the age of 21 and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more, or which involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose.

³⁹ The consideration of an *authorisation* by the *senior authorising officer* is only to be regarded as not reasonably practicable (within the meaning of section 34(2) of the 2000 Act) if he or she is on annual leave, is absent from the office and home, or is for some reason not able within a reasonable time to obtain access to a secure telephone or fax machine. Pressure of work is not normally to be regarded as rendering it impracticable for a *senior authorising officer* to consider an *application*. Where a designated deputy gives an *authorisation* this should be made clear and the reason for the absence of the *senior authorising officer* given.

Urgent cases

6.6 The *senior authorising officer* or designated deputy should generally give *authorisations* in writing. However, in urgent cases, oral *authorisations* may be given by the *senior authorising officer* or designated deputy. In an urgent oral case, a statement that the *senior authorising officer* or designated deputy has expressly authorised the conduct should be recorded in writing by the applicant as soon as is reasonably practicable, together with the information detailed below.

6.7 In an urgent case, where it is not reasonably practicable having regard to the urgency of the case for either the *senior authorising officer* or the designated deputy to consider the *application*, an *authorisation* may be granted in writing by a person entitled to act only in urgent cases under section 34(4) of the 2000 Act.⁴⁰

6.8 A case is not normally to be regarded as urgent unless the time that would elapse before the *authorising officer* was available to grant the *authorisation* would, in the judgement of the person giving the *authorisation*, be likely to endanger life or jeopardise the investigation or operation for which the *authorisation* was being given. An *authorisation* is not to be regarded as urgent where the need for an *authorisation* has been neglected or the urgency is of the *authorising officer's* or *applicant's* own making.

Jurisdictional considerations

6.9 A police or NCA *authorisation* cannot be granted unless the *application* is made by a *member* of the same force or agency, unless, in the case of the police, a relevant collaboration agreement has been made (see above, on collaborative working). An HMRC or CMA *authorisation* cannot be granted unless the *application* is made by an *officer* of Revenue and Customs or CMA respectively.

⁴⁰ Note that out-of-hours *officers* of assistant chief constable rank or above will be entitled to act for this purpose.

6.10 Where the surveillance is carried out in relation to any residential premises, the *authorisation* cannot be granted unless the residential premises are in the same area of operation of the force or organisation, unless, in the case of the police, a relevant collaboration agreement has been made (see above, on collaborative working).

Approval of Surveillance Commissioners

6.11 Except in urgent cases a police, NCA, HMRC or CMA *authorisation* granted for intrusive surveillance will not take effect until it has been approved by a Surveillance Commissioner and written notice of the Commissioner's decision has been given to the person who granted the *authorisation*. This means that the approval will not take effect until the notice has been received in the office of the person who granted the *authorisation* within the relevant force or organisation.

6.12 When the *authorisation* is urgent it will take effect from the time it is granted provided notice is given to the Surveillance Commissioner in accordance with section 35(3)(b) (see section 36(3) of the 2000 Act).

6.13 There may be cases that become urgent after approval has been sought but before a response has been received from a Surveillance Commissioner. In such a case, the *authorising officer* should notify the Surveillance Commissioner that the case is now urgent (pointing out that it has become urgent since the notification). In these cases, the *authorisation* will take effect immediately.

Notifications to Surveillance Commissioners

6.14 Where a person grants, renews or cancels an *authorisation* for intrusive surveillance, he or she must, as soon as is reasonably practicable, give notice in writing to a Surveillance Commissioner, where relevant, in accordance with whatever arrangements have been made by the Chief Surveillance Commissioner.⁴¹

⁴¹ The information to be included in the notification to the Surveillance Commissioner is set out in the Regulation of Investigatory Powers (Notification of *Authorisations* etc.) Order 2000; SI No. 2563.

6.15 In urgent cases, the notification must specify the grounds on which the case is believed to be one of urgency. The urgency provisions should not be used routinely. If the Surveillance Commissioner is satisfied that there were no grounds for believing the case to be one of urgency, he or she has the power to quash the *authorisation*.

Authorisation procedures for Secretary of State authorisations

6.16 Intrusive surveillance by any of the intelligence services, the Ministry of Defence or HM Forces⁴² requires the approval of a *Secretary of State*, unless these bodies are acting on behalf of another *public authority* that has obtained an *authorisation*.

6.17 Any *member* or official of the intelligence services, the Ministry of Defence and HM Forces can apply to the *Secretary of State* for an intrusive surveillance *authorisation*. *Applications* to the *Secretary of State* should specify those matters listed below.

6.18 Intelligence services *authorisations* must be made by issue of a *warrant*. Such *warrants* will generally be given in writing by the *Secretary of State*. In urgent cases, a *warrant* may be signed (but not renewed) by a senior official, with the express *authorisation* of the *Secretary of State*.

Information to be provided in all applications for intrusive surveillance

6.19 *Applications* should be in writing (unless urgent) and should describe the conduct to be authorised and the purpose of the investigation or operation. The *application* should specify:

- the reasons why the *authorisation* is necessary in the particular case and on the grounds (e.g. for the purpose of preventing or detecting serious crime) listed in section 32(3) of the 2000 Act;
- the nature of the surveillance;

⁴² Or any other *public authority* designated for this purpose under section 41(1) of the 2000 Act, such as the Home Office on the *application* of a *member* of HM Prison Service (SI 1126; 2001).

- the residential premises or private vehicle in relation to which the surveillance will take place, where known;
- the identities, where known, of those to be the subject of the surveillance;
- an explanation of the information which it is desired to obtain as a result of the surveillance;
- details of any potential collateral intrusion and why the intrusion is justified;
- details of any *confidential information* that is likely to be obtained as a consequence of the surveillance;
- the reasons why the surveillance is considered proportionate to what it seeks to achieve;
- a record should be made of whether the *authorisation* was given or refused, by whom and the time and date at which this happened.

6.20 In urgent cases, the above information may be supplied orally. In such cases the applicant should also record the following information in writing, as soon as is reasonably practicable (it is not necessary to record further detail):

- the identities, where known, of those subject to surveillance;
- the nature and location of the surveillance;
- the reasons why the *authorising officer* or the *officer* entitled to act in urgent cases considered the case so urgent that an oral instead of a written *authorisation* was given; and/or
- the reasons why it was not reasonably practicable for the *application* to be considered by the *authorising officer*.

Duration of intrusive surveillance authorisations – Secretary of State warrants for the intelligence services

6.21 A *warrant* issued by the *Secretary of State* will cease to have effect at the end of a period of six months beginning with the day on which it was issued. So an *authorisation* given at 09.00 on 12 February will expire on 11 August. (*Authorisations* (except those granted under urgency provisions) will cease at 23.59 on the last day).

6.22 *Warrants* expressly authorised by a *Secretary of State*, but signed by a senior official under the urgency procedures, will cease to have effect at the end of the second working day following the day of issue of the *warrant* unless renewed by the *Secretary of State*.

Duration of intrusive surveillance authorisations – all other intrusive surveillance authorisations

6.23 A written *authorisation* granted by a *Secretary of State*, a *senior authorising officer* or a designated deputy will cease to have effect (unless renewed) at the end of a period of three months, beginning with the day on which it took effect. So an *authorisation* given at 09.00 on 12 February will expire on 11 May. (*Authorisations* (except those lasting for 72 hours) will cease at 23.59 on the last day).

6.24 Oral *authorisations* given in urgent cases by a *Secretary of State*, a *senior authorising officer* or designated deputy, and written *authorisations* given by those only entitled to act in urgent cases, will cease to have effect (unless renewed) at the end of the period of 72 hours beginning with the time when they took effect.

Renewals of intrusive surveillance authorisations – Secretary of State authorisations

6.25 If at any time before an intelligence service *warrant* expires, the *Secretary of State* considers it necessary for the *warrant* to be renewed for the purpose for which it was issued, the *Secretary of State* may renew it in writing for a further period of six months, beginning with the day on which it would have ceased to have effect, but for the renewal.

6.26 If at any time before a *warrant* issued by a *Secretary of State* for any other *public authority* expires, the *Secretary of State* considers it necessary for the *warrant* to be renewed for the purpose for which it was issued, he or she may renew it in writing for a further period of three months, beginning with the day on which it would have ceased to have effect, but for the renewal.

Renewals of intrusive surveillance authorisations – all other intrusive surveillance authorisations

6.27 If, at any time before an *authorisation* expires, the *senior authorising officer* or, in their absence, the designated deputy considers that the *authorisation* should continue to have effect for the purpose for which it was issued, he or she may renew it in writing for a further period of three months.

6.28 As with the initial *authorisation*, the *senior authorising officer* must (unless it is a case to which the urgency procedure applies) seek the approval of a Surveillance Commissioner. The renewal will not take effect until the notice of the Surveillance Commissioner's approval has been received in the office of the person who granted the *authorisation* within the relevant force or organisation (but not before the day on which the *authorisation* would have otherwise ceased to have effect).

6.29 In urgent cases, a renewal can take effect immediately (provided this is not before the day on which the *authorisation* would have otherwise ceased to have effect). See section 35 and 36 of the 2000 Act and the Regulation of Investigatory Powers (Notification of *Authorisations* etc.) Order 2000; SI No. 2563.

Information to be provided for all renewals of intrusive surveillance authorisations

6.30 All *applications* for a renewal of an intrusive surveillance *authorisation* or *warrant* should record:

- whether this is the first renewal or every occasion on which the *warrant/authorisation* has been renewed previously;
- any significant changes to the information listed in paragraph 6.19;
- the reasons why it is necessary to continue with the intrusive surveillance;
- the content and value to the investigation or operation of the product so far obtained by the surveillance;
- the results of any reviews of the investigation or operation (see below).

6.31 *Authorisations* may be renewed more than once, if necessary, and details of the renewal should be centrally recorded (see Chapter 8).

Cancelleds of intrusive surveillance activity

6.32 The *senior authorising officer* who granted or last renewed the *authorisation* must cancel it, or the person who made the *application* to the *Secretary of State* must apply for its cancellation, if he or she is satisfied that the surveillance no longer meets the criteria upon which it was authorised. Where the *senior authorising officer* or person who made the *application* to the *Secretary of State* is no longer available, this duty will fall on the person who has taken over the role of *senior authorising officer* or taken over from the person who made the *application* to the *Secretary of State* or the person who is acting as the *senior authorising officer*.⁴³

6.33 As soon as the decision is taken that intrusive surveillance should be discontinued, the instruction must be given to those involved to stop the intrusive surveillance. The date the *authorisation* was cancelled should be centrally recorded and documentation of any instruction to cease surveillance should be retained (see Chapter 8). There is no requirement to record any further details. However, effective practice suggests that a record should be retained detailing the product obtained from the surveillance and whether or not objectives were achieved.

6.34 Following the cancellation of any intrusive surveillance *authorisation*, other than one granted by the *Secretary of State*, the Surveillance Commissioners must be notified of the cancellation.⁴⁴

Authorisations quashed by a Surveillance Commissioner

6.35 In cases where a police, NCA, HMRC or CMA *authorisation* is quashed or cancelled by a Surveillance Commissioner, the *senior authorising officer* must immediately instruct those involved to stop

⁴³ See the Regulation of Investigatory Powers (Cancellation of *Authorisations*) Order 2000; SI No. 2794.

⁴⁴ This notification shall include the information specified in the Regulation of Investigatory Powers (Notification of *Authorisations* etc.) Order 2000; SI No. 2563.

carrying out the intrusive surveillance. Documentation of the date and time when such an instruction was given should be retained for at least three years (see Chapter 8).

Chapter 7

AUTHORISATION PROCEDURES FOR PROPERTY INTERFERENCE

General basis for lawful activity

7.1 *Authorisations* under section 5 of the 1994 Act or Part III of the 1997 Act should be sought wherever *members* of the intelligence services, the police, the *services police*, NCA, HMRC or CMA, or persons acting on their behalf, conduct entry on, or interference with, property or with wireless telegraphy that would be otherwise unlawful.

7.2 For the purposes of this chapter, ‘property interference’ shall be taken to include entry on, or interference with, property or with wireless telegraphy.

7.3 In many cases an operation using covert techniques may involve both directed or intrusive surveillance and property interference. This can be authorised as a combined *authorisation*, although the criteria for *authorisation* of each activity must be considered separately (see above, on combined *authorisations*).

Example: The use of a surveillance device for providing information about the location of a vehicle may involve some physical interference with that vehicle as well as subsequent directed surveillance activity. Such an operation could be authorised by a combined authorisation for property interference (under Part III of the 1997 Act) and, where appropriate, directed surveillance (under the 2000 Act). In this case, the necessity and proportionality of the property interference element of the authorisation would need to be considered by the appropriate authorising officer separately to the necessity and proportionality of obtaining private information by means of the directed surveillance.

7.4 A property interference *authorisation* is not required for entry (whether for the purpose of covert recording or for any other legitimate purpose) into areas open to the public in shops, bars, restaurants, hotel foyers, blocks of flats or any other premises to which, with the implied consent of the occupier, members of the public are afforded unqualified access. Nor is *authorisation* required for entry on any other land or premises at the invitation of the occupier. This is so whatever the purposes for which the premises are used. If consent for entry has been obtained by deception (e.g. requesting entry for a false purpose), however, an *authorisation* for property interference should be obtained.

Informed consent

7.5 *Authorisations* under the 1994 Act and 1997 Act are not necessary where the *public authority* is acting with the informed consent of a person able to give permission in respect of the relevant property and actions. However, consideration should still be given to the need to obtain a directed or intrusive surveillance *authorisation* under Part II of the 2000 Act depending on the operation.

Example: A vehicle is fitted with a security alarm to ensure the safety of an undercover officer. If the consent of the vehicle's owner is obtained to install this alarm, no authorisation under the 1997 Act is required. However, if the owner has not provided consent, an authorisation will be required to render lawful the property interference. The fact that the undercover officer is aware of the alarm installation is not relevant to the lawfulness of the property interference.

Incidental property interference

7.6 The 2000 Act provides that no person shall be subject to any civil liability in respect of any conduct which is incidental to correctly authorised directed or intrusive surveillance activity and for which an *authorisation* or *warrant* is not capable of being granted or might not reasonably have been expected to have been sought under any existing legislation.⁴⁵ Thus a person shall not, for example, be subject to civil liability for trespass where that trespass is incidental to properly authorised directed or intrusive surveillance activity and where an *authorisation* under the 1994 Act or 1997 Act is available but might not reasonably have been expected to be sought (perhaps due to the unforeseeable nature or location of the activity).

7.7 Where an *authorisation* for the incidental conduct is not available (for example because the 1994 Act or 1997 Act do not apply to the *public authority* in question), the *public authority* shall not be subject to civil liability in relation to any incidental conduct, by virtue of section 27(2) of the 2000 Act. Where, however, a *public authority* is capable of obtaining an *authorisation* for the activity, it should seek one wherever it could be reasonably expected to do so.

⁴⁵ See section 27(2) of the Act.

Example: Surveillance officers crossing an area of land covered by an authorisation under the 1997 Act are forced to temporarily and momentarily cross into neighbouring land to bypass an unforeseen obstruction, before returning to their authorised route.

Samples

7.8 The acquisition of samples, such as DNA samples, fingerprints and footwear impressions, where there is no consequent loss of or damage to property does not of itself constitute unlawful property interference. However, wherever it is necessary to conduct otherwise unlawful property interference to access and obtain these samples, an *authorisation* under the 1994 or 1997 Act would be appropriate. An *authorisation* for directed or intrusive surveillance would not normally be relevant to any subsequent information, whether private or not, obtained as a result of the covert technique. Once a DNA sample, fingerprint or footwear impression has been obtained, any subsequent analysis of this information will not be surveillance as defined at section 48(2) of the 2000 Act. The appropriate lawful authority in these cases is likely to be the Data Protection Act.

Example 1: Police wish to take fingerprints from a public telephone to identify a suspected criminal who is known recently to have used the telephone. The act of taking the fingerprints would not involve any unlawful property interference so no authorisation under the 1994 or 1997 Act is required. The subsequent recording and analysis of the information obtained to establish the individual's identity would not amount to surveillance and therefore would not require authorisation under the 2000 Act.

Example 2: Police intend to acquire covertly a mobile telephone used by a suspected criminal, in order to take fingerprints. In this case, the acquisition of the telephone for the purposes of obtaining fingerprints could be authorised under the 1994 or 1997 Act where it would otherwise be unlawful.

Authorisations for property interference by the police, the services police, NCA, HMRC and CMA

7.9 Responsibility for these *authorisations* rests with the *authorising officer* as defined in section 93(5) of the 1997 Act, i.e. the chief constable or equivalent. *Authorisations* require the personal authority of the *authorising officer* (or their designated deputy) except in urgent situations, where it is not reasonably practicable for the *application* to be considered by such person. The person entitled to act in such cases is set out in section 94 of the 1997 Act.

7.10 Any person giving an *authorisation* for entry on or interference with property or with wireless telegraphy under section 93(2) of the 1997 Act must believe that:

- it is necessary for the action specified to be taken for the purpose of preventing or detecting serious crime;⁴⁶ and
- that the taking of the action is proportionate to what the action seeks to achieve.

7.11 The *authorising officer* must take into account whether what it is thought necessary to achieve by the authorised conduct could reasonably be achieved by other means.

⁴⁶ An *authorising officer* in a *public authority* other than the Security Service shall not issue an *authorisation* under Part III of the 1997 Act where the investigation or operation falls within the responsibilities of the Security Service. Where any doubt exists a *public authority* should confirm with the Security Service whether or not the investigation is judged to fall within Security Service responsibilities before seeking an *authorisation* under Part III of the 1997 Act. Where the *authorising officer* is the Chair of the CMA, the only purpose falling within this definition is the purpose of preventing or detecting an offence under section 188 of the Enterprise Act 2002 (see section 93(2AA) of the 1997 Act.

Collaborative working and regional considerations

7.12 *Authorisations* for the police, the *services police*, NCA, HMRC and CMA may only be given by an *authorising officer* on *application* by a *member* or *officer* of the same force or agency unless, in the case of the police, a relevant collaboration agreement has been made which permits this rule to be varied.

7.13 *Authorisations* for the police may only be given for property interference within the *authorising officer's* own area of operation unless, in the case of the police, a relevant collaboration agreement has been made which permits this rule to be varied. Unless a relevant collaboration agreement applies, an *authorising officer* may authorise property interference (excluding wireless telegraphy interference) outside the relevant area, solely for the purpose of maintaining (including replacing) or retrieving any device, apparatus or equipment the use of which within the relevant area has been authorised under the 1997 Act or 2000 Act. Unless a relevant collaboration agreement applies, an *authorisation* for maintenance or retrieval outside of the *authorising officer's* own area of operations can only be given for circumstances that do not require entry onto private land.

7.14 Any person granting or applying for an *authorisation* or *warrant* to enter on or interfere with property or with wireless telegraphy will also need to be aware of particular sensitivities in the local community where the entry or interference is taking place and of similar activities being undertaken by other *public authorities* which could impact on the deployment. In this regard, it is recommended that the *authorising officers* in the *services police*, NCA, HMRC and CMA should consult a senior *officer* within the police force in which the investigation or operation takes place where the *authorising officer* considers that conflicts might arise. The Chief Constable of the Police Service of Northern Ireland should be informed of any surveillance operation undertaken by another law enforcement agency which involves its *officers* maintaining (including replacing) or retrieving equipment in Northern Ireland.

Authorisation procedures

7.15 *Authorisations* will generally be given in writing by the *authorising officer*. However, in urgent cases, they may be given orally by the *authorising officer*. In such cases, a statement that the *authorising officer* has expressly authorised the action(s) should be recorded in writing by the applicant as soon as is reasonably practicable, together with that information detailed below.

7.16 If the *authorising officer* is absent then an *authorisation* can be given in writing or, in urgent cases, orally by the designated deputy as provided for in section 94(4) of the 1997 Act, section 12(A) of the Police Act 1996, section 18 of the Police and Fire Reform (Scotland) Act 2012, section 25 of the City of London Police Act 1839 or section 93(5) of the 1997 Act (for NCA).

7.17 Where, however, in an urgent case, it is not reasonably practicable for the *authorising officer* or designated deputy to consider an *application*, then written *authorisation* may be given by the following:

- in the case of the police, by an assistant chief constable (other than a designated deputy);⁴⁷
- in the case of the Metropolitan Police and City of London Police, by a commander;
- in the case of MOD police or British Transport Police, by a deputy or assistant chief constable;
- in the case of the *services police*, by an assistant Provost Marshal (in the Royal Naval Police) or deputy Provost Marshal (in the Royal Military Police or Royal Air Force Police);
- in the case of NCA a person designated by the Director General;
- in the case of HMRC, by a person designated by the Commissioners of Revenue and Customs;⁴⁸
- in the case of the CMA, by an *officer* of the CMA designated for this purpose.

⁴⁷ ACPO out-of-hours *officers* of assistant chief constable rank or above will be entitled to act for this purpose.

⁴⁸ This will be an *officer* of the rank of assistant chief investigation *officer*.

Information to be provided in applications

7.18 *Applications* to the *authorising officer* for the granting or renewal of an *authorisation* must be made in writing (unless urgent) by a police *officer*, Revenue and Customs *officer*, a *member* of NCA or an *officer* of the CMA and should specify:

- the identity or identities, where known, of those who possess the property that is to be subject to the interference;
- sufficient information to identify the property which the entry or interference with will affect;
- the nature and extent of the proposed interference;
- the details of any collateral intrusion, including the identity of individuals and/or categories of people, where known, who are likely to be affected, and why the intrusion is justified;
- details of the offence suspected or committed;
- how the *authorisation* criteria (as set out above) have been met;
- any action which may be necessary to maintain any equipment, including replacing it;
- any action which may be necessary to retrieve any equipment;
- in case of a renewal, the results obtained so far, or a full explanation of the failure to obtain any results; and
- whether an *authorisation* was given or refused, by whom and the time and date on which this happened.

7.19 In urgent cases, the above information may be supplied orally. In such cases the *authorising officer* and the applicant should also record the following information in writing, as soon as is reasonably practicable (it is not necessary to record further detail):

- the identity or identities of those owning or using the property (where known);
- sufficient information to identify the property which will be affected;
- details of the offence suspected or committed;
- the reasons why the *authorising officer* or designated deputy considered the case so urgent that an oral instead of a written *authorisation* was given; and/or

- the reasons why (if relevant) it was not reasonably practicable for the *application* to be considered by the *authorising officer* or the designated deputy.

Notifications to Surveillance Commissioners

7.20 Where a person gives, renews or cancels an *authorisation* in respect of entry on or interference with property or with wireless telegraphy, he or she must, as soon as is reasonably practicable, give notice of it in writing to a Surveillance Commissioner, where relevant, in accordance with arrangements made by the Chief Surveillance Commissioner. In urgent cases which would otherwise have required the approval of a Surveillance Commissioner, the notification must specify the grounds on which the case is believed to be one of urgency.

7.21 There may be cases which become urgent after approval has been sought but before a response has been received from a Surveillance Commissioner. In such a case, the *authorising officer* should notify the Surveillance Commissioner that the case is urgent (pointing out that it has become urgent since the previous notification). In these cases, the *authorisation* will take effect immediately.

7.22 Notifications to Surveillance Commissioners in relation to the granting, renewal and cancellation of *authorisations* in respect of entry on or interference with property should be in accordance with the requirements of the Police Act 1997 (Notifications of *Authorisations* etc.) Order 1998; SI No. 3241.

Cases requiring prior approval of a Surveillance Commissioner

7.23 In certain cases, an *authorisation* for entry on or interference with property will not take effect until a Surveillance Commissioner has approved it and the notice of approval has been received in the office of the person who granted the *authorisation* within the relevant force or organisation (unless the urgency procedures are used). These are cases where the person giving the *authorisation* believes that:

- any of the property specified in the *authorisation*:
 - is used wholly or mainly as a dwelling or as a bedroom in a hotel; or
 - constitutes office premises;⁴⁹ or
- the action authorised is likely to result in any person acquiring knowledge of:
 - matters subject to *legal privilege*;
 - confidential personal information; or
 - confidential journalistic material.

Duration of authorisations

7.24 Written *authorisations* in respect of entry on or interference with property or with wireless telegraphy given by *authorising officers* will cease to have effect at the end of a period of three months beginning with the day on which they took effect. So an *authorisation* given at 09.00 on 12 February will expire on 11 May. (*Authorisations* (except those lasting for 72 hours) will cease at 23.59 on the last day).

7.25 In cases requiring prior approval by a Surveillance Commissioner, the duration of an *authorisation* is calculated from the time at which the person who gave the *authorisation* was notified that the Surveillance Commissioner had approved it. This can be done by presenting the *authorising officer* with the approval decision page to note in person or if the *authorising officer* is unavailable, sending the written notice by auditable electronic means. In cases not requiring prior approval, this means from the time the *authorisation* was granted.

7.26 Written *authorisations* given by the persons specified in 7.16 (section 94 of the 1997 Act) and oral *authorisations* given in urgent cases by:

- *authorising officers*; or
- designated deputies

⁴⁹ Office premises are defined as any building or part of a building whose sole or principal use is as an office or for office purposes (which means purposes of administration, clerical work, handling money and telephone or telegraph operation).

will cease at the end of the period of 72 hours beginning with the time when they took effect.

Renewals

7.27 If at any time before the time and day on which an *authorisation* expires the *authorising officer* or, in their absence, the designated deputy considers the *authorisation* should continue to have effect for the purpose for which it was issued, he or she may renew it in writing for a period of three months beginning with the day on which the *authorisation* would otherwise have ceased to have effect. *Authorisations* may be renewed more than once, if necessary, and details of the renewal should be centrally recorded (see Chapter 8).

7.28 Where relevant, the Commissioners must be notified of renewals of *authorisations*. The information to be included in the notification is set out in the Police Act 1997 (Notifications of *Authorisations* etc.) Order 1998; SI No. 3241.

7.29 If, at the time of renewal, criteria exist which would cause an *authorisation* to require prior approval by a Surveillance Commissioner, then the approval of a Surveillance Commissioner must be sought before the renewal can take effect. The fact that the initial *authorisation* required the approval of a Commissioner before taking effect does not mean that its renewal will automatically require such approval. It will only do so if, at the time of the renewal, it falls into one of the categories requiring approval (and is not an urgent case).

Cancellations

7.30 The *senior authorising officer* who granted or last renewed the *authorisation* must cancel it if he or she is satisfied that the *authorisation* no longer meets the criteria upon which it was authorised. Where the *senior authorising officer* is no longer available, this duty will fall on the person who has taken over the role of *senior authorising officer* or the person who is acting as the *senior authorising officer* (see the Regulation of Investigatory Powers (Cancellation of *Authorisations*) Order 2000; SI No. 2794).

7.31 Following the cancellation of the *authorisation*, the Surveillance Commissioners must be notified of the cancellation. The information to be included in the notification is set out in the Police Act 1997 (Notifications of *Authorisations* etc.) Order 1998; SI No. 3421.

7.32 The Surveillance Commissioners have the power to cancel an *authorisation* if they are satisfied that, at any time after an *authorisation* was given or renewed, there were no reasonable grounds for believing that it should subsist. In such circumstances, a Surveillance Commissioner may order the destruction of records, in whole or in part, other than any that are required for pending criminal or civil proceedings.

Retrieval of equipment

7.33 Because of the time it can take to remove equipment from a person's property it may also be necessary for an *authorisation* to make clear that it also permits the retrieval of anything left on property following completion of the intended action. The notification to Commissioners of the authorisation should include reference to the need to remove the equipment and, where possible, a timescale for removal.

7.34 Where a Surveillance Commissioner quashes or cancels an *authorisation* or renewal, he or she will, if there are reasonable grounds for doing so, order that the *authorisation* remain effective for a specified period, to enable *officers* to retrieve anything left on the property by virtue of the *authorisation*. He or she can only do so if the *authorisation* or renewal makes provision for this. A decision by the Surveillance Commissioner not to give such an order can be the subject of an appeal to the Chief Surveillance Commissioner.

Ceasing of entry on or interference with property or with wireless telegraphy

7.35 Once an *authorisation* or renewal expires or is cancelled or quashed, the *authorising officer* must immediately give an instruction to cease all the actions authorised for the entry on or interference with

property or with wireless telegraphy. The time and date when such an instruction was given should be centrally retrievable for at least three years (see Chapter 8).

Authorisations for property interference by the intelligence services

7.36 An *application* for a *warrant* must be made by a *member* of the intelligence services for the taking of action in relation to that agency. In addition, the Security Service may make an *application* for a *warrant* to act on behalf of the Secret Intelligence Service (SIS) and the Government Communications Headquarters (GCHQ). SIS and GCHQ may not be granted a *warrant* for action in support of the prevention or detection of serious crime which relates to property in the British Islands.

7.37 The intelligence services should provide the same information as other agencies, as and where appropriate, when making *applications* for the grant or renewal of property *warrants*.

7.38 Before granting a *warrant*, the *Secretary of State* must:

- think it necessary for the action to be taken for the purpose of assisting the relevant agency in carrying out its functions;
- be satisfied that the taking of the action is proportionate to what the action seeks to achieve;
- take into account in deciding whether an *authorisation* is necessary and proportionate whether the information which it is thought necessary to obtain by the conduct authorised by the *warrant* could reasonably be obtained by other means; and
- be satisfied that there are satisfactory arrangements in force under the 1994 Act or the 1989 Act in respect of disclosure of any material obtained by means of the *warrant*, and that material obtained will be subject to those arrangements.

Renewals of intelligence services warrants

7.39 A *warrant* shall, unless renewed, cease to have effect at the end of the period of six months beginning with the day on which it was issued (if the *warrant* was issued under the hand of the *Secretary of State*) or at the end of the period ending with the fifth working day following the day on which it was issued (in any other case).

7.40 If at any time before the day on which a *warrant* would cease to have effect the *Secretary of State* considers it necessary for the *warrant* to continue to have effect for the purpose for which it was issued, he or she may by an instrument under his or her hand renew it for a period of six months beginning with the day it would otherwise cease to have effect.

Cancellations of intelligence services warrants

7.41 The *Secretary of State* shall cancel a *warrant* if he or she is satisfied that the action authorised by it is no longer necessary.

7.42 The person who made the *application* to the *Secretary of State* must apply for its cancellation, if he or she is satisfied that the *warrant* no longer meets the criteria upon which it was authorised. Where the person who made the *application* to the *Secretary of State* is no longer available, this duty will fall on the person who has taken over from the person who made the *application* to the *Secretary of State* (see the Regulation of Investigatory Powers (Cancellation of *Authorisations*) Order 2000; SI No. 2794).

Retrieval of equipment by the intelligence services

7.43 Because of the time it can take to remove equipment from a person's property it may also be necessary to renew a property *warrant* in order to complete the retrieval. *Applications* to the *Secretary of State* for renewal should state why it is being or has been closed down, why it has not been possible to remove the equipment and any timescales for removal, where known.

Chapter 8

KEEPING OF RECORDS

Centrally retrievable records of authorisations

Directed and intrusive surveillance authorisations

8.1 A record of the following information pertaining to all *authorisations* shall be centrally retrievable within each *public authority* for a period of at least three years from the ending of each *authorisation*.⁵⁰ This information should be regularly updated whenever an *authorisation* is granted, renewed or cancelled and should be made available to the relevant Commissioner or an Inspector from the Office of Surveillance Commissioners upon request. More guidance for local authorities on the recording of magistrates' decisions is available in Home Office-issued guidance available on the gov.uk website.

- the type of *authorisation*;
- the date the *authorisation* was given;
- name and rank/grade of the *authorising officer*;
- the unique reference number (URN) of the investigation or operation;
- the title of the investigation or operation, including a brief description and names of subjects, if known;
- whether the urgency provisions were used, and if so why;
- for local authorities, details of attendances at the magistrates' court to include the date of attendances at court, the determining magistrate, the decision of the court and the time and date of that decision;
- the dates of any reviews;

⁵⁰ See also paragraph 8.4.

- if the *authorisation* has been renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the *authorising officer*;
- whether the investigation or operation is likely to result in obtaining *confidential information* as defined in this code of practice;⁵¹
- whether the *authorisation* was granted by an individual directly involved in the investigation;⁵²
- the date the *authorisation* was cancelled.

8.2 The following documentation should also be centrally retrievable for at least three years from the ending of each *authorisation*:

- a copy of the *application* and a copy of the *authorisation* together with any supplementary documentation and notification of the approval given by the *authorising officer*;
- a record of the period over which the surveillance has taken place;
- the frequency of reviews prescribed by the *authorising officer*;
- a record of the result of each review of the *authorisation*;
- a copy of any renewal of an *authorisation*, together with the supporting documentation submitted when the renewal was requested;
- the date and time when any instruction to cease surveillance was given;
- the date and time when any other instruction was given by the *authorising officer*;
- for local authorities a copy of the order approving or otherwise the grant or renewal of an authorisation from a Justice of the Peace (JP).

51 See Chapter 4.

52 See paragraph 5.7.

Property interference authorisations

8.3 The following information relating to all *authorisations* for property interference should be centrally retrievable for at least three years:⁵³

- the time and date when an *authorisation* is given;
- whether an *authorisation* is in written or oral form;
- the time and date when it was notified to a Surveillance Commissioner, if applicable;
- the time and date when the Surveillance Commissioner notified his or her approval (where appropriate);
- every occasion when entry on or interference with property or with wireless telegraphy has occurred;
- the result of periodic reviews of the *authorisation*;
- the date of every renewal; and
- the time and date when any instruction was given by the *authorising officer* to cease the interference with property or with wireless telegraphy.

8.4 RIPA records must be available for inspection by the Commissioner and retained to allow the Investigatory Powers Tribunal, established under Part IV of the Act, to carry out its functions. The Tribunal will consider complaints made up to one year after the conduct to which the complaint relates and, where it is equitable to do so, may consider complaints made more than one year after the conduct to which the complaint relates (see section 67(5) of the Act), particularly where continuing conduct is alleged. Although records are only required to be retained for at least three years, it is therefore desirable, if possible, to retain records for up to five years.

⁵³ See also paragraph 8.4.

Chapter 9

HANDLING OF MATERIAL AND USE OF MATERIAL AS EVIDENCE

Use of material as evidence

9.1 Subject to the provisions in Chapter 4 of this code, material obtained through directed or intrusive surveillance, or entry on, or interference with, property or wireless telegraphy, may be used as evidence in criminal proceedings. The admissibility of evidence is governed primarily by the common law, the Civil Procedure Rules, section 78 of the Police and Criminal Evidence Act 1984⁵⁴ and the Human Rights Act 1998.

9.2 Any decisions by a Surveillance Commissioner in respect of granting prior approval for intrusive surveillance activity or entry on, or interference with, property or with wireless telegraphy, shall not be subject to appeal or be liable to be questioned in any court.⁵⁵

Retention and destruction of material

9.3 Each *public authority* must ensure that arrangements are in place for the secure handling, storage and destruction of material obtained through the use of directed or intrusive surveillance or property interference. *Authorising officers*, through their relevant data controller, must ensure compliance with the appropriate data protection requirements under the Data Protection Act 1998 and any relevant codes of practice produced by individual authorities relating to the handling and storage of material.

⁵⁴ And section 76 of the Police & Criminal Evidence (Northern Ireland) Order 1989.

⁵⁵ See section 91(10) of the 1997 Act.

9.4 Where the product of surveillance or interference with property or wireless telegraphy could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements⁵⁶ for a suitable further period, commensurate to any subsequent review.

9.5 There is nothing in the 2000 Act, 1994 Act or 1997 Act which prevents material obtained under directed or intrusive surveillance or property interference *authorisations* from being used to further other investigations.

Law enforcement agencies

9.6 In the cases of the law enforcement agencies, particular attention is drawn to the requirements of the code of practice issued under the Criminal Procedure and Investigations Act 1996. This requires that material which is obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained.

The intelligence services, MOD and HM Forces

9.7 The heads of these agencies are responsible for ensuring that arrangements exist for securing that no information is stored by the authorities, except as necessary for the proper discharge of their functions. They are also responsible for arrangements to control onward disclosure. For the intelligence services, this is a statutory duty under the 1989 Act and the 1994 Act.

9.8 With regard to the service police forces (the Royal Navy Police, the Royal Military Police and the Royal Air Force Police), particular attention is drawn to the Criminal Procedure and Investigations Act 1996 (Code of Practice) (Armed Forces) Order 2008, which requires that the investigator retain all material obtained in a service investigation which may be relevant to the investigation.

⁵⁶ For example, under the Criminal Procedure and Investigations Act 1996.

Chapter 10

OVERSIGHT BY COMMISSIONERS

10.1 The 1997 and 2000 Acts require the Chief Surveillance Commissioner to keep under review (with the assistance of the Surveillance Commissioners and Assistant Surveillance Commissioners) the performance of functions under Part III of the 1997 Act and Part II of the 2000 Act by the police (including the service police forces, the Ministry of Defence Police and the British Transport Police), NCA, HMRC and the other *public authorities* listed in Schedule 1 of the 2000 Act and the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 and, in Northern Ireland, officials of the Ministry of Defence and HM Forces.

10.2 The Intelligence Services Commissioner's remit is to provide independent oversight of the use of the powers contained within Part II of the 2000 Act and the 1994 Act by the Security Service, Secret Intelligence Service, GCHQ and the Ministry of Defence and HM Forces (excluding the service police forces, and in Northern Ireland officials of the Ministry of Defence and HM Forces).

10.3 This code does not cover the exercise of any of the Commissioners' functions. It is the duty of any person who uses these powers to comply with any request made by a Commissioner to disclose or provide any information he or she requires for the purpose of enabling the Commissioner to carry out their functions.

10.4 References in this code to the performance of review functions by the Chief Surveillance Commissioner and other Commissioners apply also to Inspectors and other *members* of staff to whom such functions have been delegated.

Chapter 11

COMPLAINTS

11.1 The 2000 Act establishes an independent Tribunal. This Tribunal will be made up of senior *members* of the judiciary and the legal profession and is independent of the Government. The Tribunal has full powers to investigate and decide any case within its jurisdiction. This code does not cover the exercise of the Tribunal's functions. Details of the relevant complaints procedure can be obtained from the following address:

Investigatory Powers Tribunal

PO Box 33220

London

SW1H 9ZQ

 020 7035 3711

Chapter 12

GLOSSARY

Application	A request made to an <i>authorising officer</i> to consider granting (or renewing) an <i>authorisation</i> for directed or intrusive surveillance (under the 2000 Act), or interference with property or wireless telegraphy (under the 1994 or 1997 Act). An <i>application</i> will be made by a <i>member</i> of a relevant <i>public authority</i> .
Authorisation	An <i>application</i> which has received the approval of an <i>authorising officer</i> . Depending on the circumstances, an <i>authorisation</i> may comprise a written <i>application</i> that has been signed by the <i>authorising officer</i> , or an oral <i>application</i> that has been verbally approved by the <i>authorising officer</i> .
Authorising officer	A person within a <i>public authority</i> who is entitled to grant <i>authorisations</i> under the 2000 or 1997 Acts or to apply to the <i>Secretary of State</i> for such <i>warrants</i> . Should be taken to include <i>senior authorising officers</i> .
Confidential information	Confidential personal information (such as medical records or spiritual counselling), confidential journalistic material, confidential discussions between <i>Members of</i>

	<p><i>Parliament</i> and their constituents, or matters subject to <i>legal privilege</i>. See Chapter 4 for a full explanation.</p>
Legal privilege	<p>Matters subject to <i>legal privilege</i> are defined in section 98 of the 1997 Act. This includes certain communications between professional legal advisers and their clients or persons representing the client.</p>
Member	<p>An employee of an organisation, or a person seconded to that organisation.</p>
Member of Parliament	<p>Is reference to a Member of both Houses of the UK Parliament, the European Parliament, the Scottish Parliament, the Welsh Assembly, and Northern Ireland Assembly.</p>
Officer	<p>An <i>officer</i> of a police force, HMRC, or the CMA, or a person seconded to one of these agencies as an <i>officer</i>.</p>
Private information	<p>Any information relating to a person in relation to which that person has or may have a reasonable expectation of privacy. This includes information relating to a person's private, family or professional affairs. <i>Private information</i> includes information about any person, not just the subject(s) of an investigation.</p>
Public authority	<p>Any public organisation, agency or police force (including the military police forces).</p>

Secretary of State	Any <i>Secretary of State</i> (in practice this will generally be the Home Secretary).
Senior authorising officer	A person within a <i>public authority</i> who is entitled to grant intrusive surveillance <i>authorisations</i> under the 2000 Act or to apply to the <i>Secretary of State</i> for such <i>warrants</i> . See also <i>Authorising officer</i> .
Services police	The Royal Naval Police, Royal Military Police or Royal Air Force Police.
Warrant	A type of <i>authorisation</i> granted by a <i>Secretary of State</i> following an <i>application</i> for intrusive surveillance or property interference under the 1994, 1997 or 2000 Acts.

Annex A

Authorisation levels when knowledge of confidential information is likely to be acquired

Relevant public authority	Authorisation level
Police Forces:	
Any police force maintained under section 2 of the Police Act 1996 (police forces in England and Wales outside London)	Chief Constable
The Police Service of Scotland	Chief Constable
The Metropolitan police force	Assistant Commissioner
The City of London police force	Commissioner
The Police Service of Northern Ireland	Deputy Chief Constable
The Ministry of Defence Police	Chief Constable
The Royal Navy Police	Provost Marshal
The Royal Military Police	Provost Marshal
The Royal Air Force Police	Provost Marshal
The National Crime Agency	Deputy Director General
The Serious Fraud Office	A Member of the Senior Civil Service or Head of Domain
The Intelligence Services:	
The Security Service	Deputy Director General

Relevant public authority	Authorisation level
The Secret Intelligence Service	A Director of the Secret Intelligence Service
The Government Communications Headquarters	A Director of GCHQ
HM Forces:	
The Royal Navy	Rear Admiral
The Army	Major General
The Royal Air Force	Air-Vice Marshal
The Commissioners for HM Revenue and Customs	Director Investigation, or Regional Heads of Investigation
The Department for Environment, Food and Rural Affairs:	
DEFRA Investigation Services	Head of DEFRA Investigation Services
Marine and Fisheries Agency	Head of DEFRA Prosecution Service
Centre for Environment, Fisheries and Aquaculture Science	Head of DEFRA Prosecution Service
The Department of Health:	
The Medicines and Healthcare Products Regulatory Agency	Chief Executive of the Medicines and Healthcare Products Regulatory Agency

Relevant public authority	Authorisation level
The Home Office	Senior Civil Service pay band 1 with responsibility for criminal investigations in relation to immigration and border security
The Ministry of Justice	Chief Executive Officer of the National Offender Management Service
The Northern Ireland Office: The Northern Ireland Prison Service	Director or Deputy Director Operations in the Northern Ireland Prison Service
The Department of Business, Innovation and Skills	The Director of Legal Services A
The Welsh Assembly Government	Head of Department for Health and Social Services, Head of Department for Health and Social Services Finance, Head of Rural Payments Division, Regional Director or equivalent grade in the Care and Social Services Inspectorate for Wales
Any county council or district council in England, a London borough council, the Common Council of the City of London in its capacity as a local authority, the Council of the Isles of Scilly, and any county council or borough council in Wales	The Head of Paid Service, or (in his/her absence) the person acting as the Head of Paid Service

Relevant public authority	Authorisation level
The Environment Agency	Chief Executive of the Environment Agency
The Prudential Regulation Authority	Chief Executive of the Prudential Regulation Authority
The Competition and Markets Authority	Chair of the Competition and Markets Authority
The Financial Conduct Authority	Chairman of the Financial Conduct Authority
The Food Standards Agency	Head of Group, or Deputy Chief Executive or Chief Executive of the Foods Standards Agency
The Health and Safety Executive	Director of Field Operations, or Director of Hazardous Installations Directorate
NHS bodies in England and Wales: A Special Health Authority established under section 28 of the National Health Service Act 2006 or section 22 of the National Health Service (Wales) Act 2006	Managing Director of the NHS Counter Fraud and Security Management Services Division of the NHS Business Services Authority
The Royal Pharmaceutical Society of Great Britain	Deputy Registrar and Director of Regulation
The Department of Work and Pensions: Jobcentre Plus	Chief Executive of Jobcentre Plus

Relevant public authority	Authorisation level
The Royal Mail Group Ltd, by virtue of being a Universal Service Provider within the meaning of the Postal Services Act 2000	Director of Security

This code of practice provides guidance and rules on authorisations for the carrying out of surveillance (directed surveillance and intrusive surveillance) under Part 2 of the Regulation of Investigatory Powers Act 2000 and for interference with property or with wireless telegraphy under Part 3 of the Police Act 1997. It sets out the various authorisation procedures to be followed for the grant, review, renewal and cancellation of authorisations, as well as special rules for authorisations in respect of confidential and legally privileged information.

The code is aimed primarily at members of public authorities involved in making applications for the grant of authorisations and those persons designated to grant authorisations.



www.tso.co.uk

ISBN 978-0-11-341373-7



9

Appendix 3



Home Office

Covert Human Intelligence Sources

Code of Practice

Pursuant to Section 71 of the Regulation of
Investigatory Powers Act 2000

Covert Human Intelligence Sources

Code of Practice

Pursuant to section 71(4) of the Regulation of
Investigatory Powers Act 2000

LONDON: TSO



information & publishing solutions

Published by TSO (The Stationery Office) and available from:

Online

www.tsoshop.co.uk

Mail, Telephone, Fax & E-mail

TSO

PO Box 29, Norwich, NR3 1GN

Telephone orders/General enquiries:

0870 600 5522

Fax orders: 0870 600 5533

E-mail: customer.services@tso.co.uk

Textphone: 0870 240 3701

TSO@Blackwell and other Accredited Agents

Published with the permission of the Home Office on behalf of the Controller of Her Majesty's Stationery Office.

© Crown Copyright 2014

All rights reserved

You may re-use this information (excluding logos) free of charge in any format or medium, under the terms of the Open Government Licence v.2. To view this licence visit www.nationalarchives.gov.uk/doc/open-government-licence/version/2/ or email PSI@nationalarchives.gsi.gov.uk. Where third-party material has been identified, permission from the respective copyright holder must be sought.

Whilst every attempt has been made to ensure that the information in this publication is up to date at the time of publication, the publisher cannot accept responsibility for any inaccuracies.

First published 2014

ISBN 978 0 11 3413744

Printed in the United Kingdom for The Stationery Office.
J002969997 C10 12/14

Contents

Chapter 1	Introduction	5
Chapter 2	Covert human intelligence sources: definitions and examples	8
Chapter 3	General rules on authorisations	16
Chapter 4	Special considerations for authorisations	24
Chapter 5	Authorisation procedures for covert human intelligence sources	34
Chapter 6	Management of covert human intelligence sources	43
Chapter 7	Keeping of records	47
Chapter 8	Handling of material	50
Chapter 9	Senior responsible officers and oversight by Commissioners	52
Chapter 10	Complaints	54
Annex A	Authorisation levels when knowledge of confidential information is likely to be acquired or when a vulnerable individual or juvenile is to be used as a source	55
Annex B	Authorisation levels for the enhanced arrangements set out in the Regulation of Investigatory Powers (Covert Human Intelligence Sources: Relevant Sources) Order 2013	62

Chapter 1

INTRODUCTION

Definitions

1.1 In this code the:

- ‘1989 Act’ means the Security Service Act 1989;
- ‘1994 Act’ means the Intelligence Services Act 1994;
- ‘1997 Act’ means the Police Act 1997;
- ‘2000 Act’ means the Regulation of Investigatory Powers Act 2000 (RIPA);
- ‘RIP(S)A’ means the Regulation of Investigatory Powers (Scotland) Act 2000;
- ‘2010 Order’ means the Regulation of Investigatory Powers (Covert Human Intelligence Sources: Matters Subject to Legal Privilege) Order 2010;
- ‘2013 Order’ means the Regulation of Investigatory Powers (Covert Human Intelligence Sources: Relevant Sources) Order 2013.

Background

1.2 This code of practice provides guidance on the authorisation of the use or conduct of covert human intelligence sources (CHIS) by public authorities under Part II of the 2000 Act.

1.3 This code is issued pursuant to section 71 of the 2000 Act, which stipulates that the Secretary of State shall issue one or more codes of practice in relation to the powers and duties in Parts I to III of the 2000 Act, section 5 of the 1994 Act and Part III of the 1997 Act. This code replaces the previous code of practice issued in 2010.

1.4 This code is publicly available and should be readily accessible by members of any relevant public authority seeking to use the 2000 Act to authorise the use or conduct of CHIS.¹

Effect of code

1.5 The 2000 Act provides that all codes of practice relating to the 2000 Act are admissible as evidence in criminal and civil proceedings. If any provision of this code appears relevant to any court or tribunal considering any such proceedings, or to the Investigatory Powers Tribunal established under the 2000 Act, or to one of the Commissioners responsible for overseeing the powers conferred by the 2000 Act, it must be taken into account. Public authorities may also be required to justify, with regard to this code, the use or granting of authorisations in general or the failure to use or grant authorisations where appropriate.

1.6 Examples are included in this code to assist with the illustration and interpretation of certain provisions. Examples are not provisions of the code, but are included for guidance only. It is not possible for theoretical examples to replicate the level of detail to be found in real cases. Consequently, authorising officers should avoid allowing superficial similarities with the examples to determine their decisions and should not seek to justify their decisions solely by reference to the examples rather than to the law, including the provisions of this code.

Scope of covert human intelligence source activity to which this code applies

1.7 Part II of the 2000 Act provides for the authorisation of the use or conduct of CHIS. The definitions of these terms are laid out in section 26 of the 2000 Act and Chapter 2 of this code.

1.8 Not all human sources of information will fall within these definitions and an authorisation under the 2000 Act will therefore not always be appropriate.

¹ Being those listed in or added to Part I of schedule 1 of the 2000 Act.

1.9 Neither Part II of the 2000 Act nor this code of practice is intended to affect the existing practices and procedures surrounding criminal participation of CHIS.

Chapter 2

COVERT HUMAN INTELLIGENCE SOURCES: DEFINITIONS AND EXAMPLES

Definition of a covert human intelligence source

2.1 Under the 2000 Act, a person is a CHIS if:

- (a) they establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph b) or c);
- (b) they covertly use such a relationship to obtain information or to provide access to any information to another person; or
- (c) they covertly disclose information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.²

2.2 A relationship is established or maintained for a covert purpose if and only if it is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.³

2.3 A relationship is used covertly, and information obtained is disclosed covertly, if and only if the relationship is used or the information is disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.⁴

2.4 The 2013 Order further defines a particular type of CHIS as a 'relevant source'. This is a source holding an office, rank or position with the public authorities listed in the Order and Annex B to this code. Enhanced authorisation arrangements are in place for this type of source as detailed in this code. Such sources will be referred to as 'relevant source' throughout this code.

2 See section 26(8) of the 2000 Act.

3 See section 26(9)(b) of the 2000 Act for full definition.

4 See section 26(9)(c) of the 2000 Act for full definition.

Scope of ‘use’ or ‘conduct’ authorisations

2.5 Subject to the procedures outlined in Chapter 3 of this code, an authorisation may be obtained under Part II of the 2000 Act for the use or conduct of CHIS.

2.6 The use of a CHIS involves any action on behalf of a public authority to induce, ask or assist a person to engage in the conduct of a CHIS, or to obtain information by means of the conduct of a CHIS.⁵ In general, therefore, an authorisation for use of a CHIS will be necessary to authorise steps taken by a public authority in relation to a CHIS.

2.7 The conduct of a CHIS is any conduct of a CHIS which falls within paragraph 2.1 above or is incidental to anything falling within that paragraph. In other words, an authorisation for conduct will authorise steps taken by the CHIS on behalf, or at the request, of a public authority.⁶

2.8 Most CHIS authorisations will be for both use and conduct. This is because public authorities usually take action in connection with the CHIS, such as tasking the CHIS to undertake covert action, and because the CHIS will be expected to take action in relation to the public authority, such as responding to particular tasking.

2.9 Care should be taken to ensure that the CHIS is clear on what is/is not authorised at any given time and that all the CHIS’s activities are properly risk assessed. Care should also be taken to ensure that relevant applications, reviews, renewals and cancellations are correctly performed. A CHIS may in certain circumstances be the subject of different use or conduct authorisations obtained by one or more public authorities. Such authorisations should not conflict.

⁵ See section 26(7)(b) of the 2000 Act.

⁶ See section 26(7)(a) of the 2000 Act.

Circumstances in which it would be appropriate to authorise the use or conduct of a CHIS

2.10 Public authorities are not required by the 2000 Act to seek or obtain an authorisation just because one is available (see section 80 of the 2000 Act). The use or conduct of a CHIS, however, can be a particularly intrusive and high-risk covert technique, requiring dedicated and sufficient resources, oversight and management. This will include ensuring that all use or conduct is:

- necessary and proportionate to the intelligence dividend that it seeks to achieve;
- in compliance with relevant Articles of the European Convention on Human Rights (ECHR), particularly Articles 6 and 8.

2.11 Unlike directed surveillance, which relates specifically to private information, authorisations for the use or conduct of a CHIS do not relate specifically to private information, but to the covert manipulation of a relationship to gain any information. ECHR case law makes it clear that Article 8 includes the right to establish and develop relationships. Accordingly, any manipulation of a relationship by a public authority (e.g. one party having a covert purpose on behalf of a public authority) is likely to engage Article 8, regardless of whether or not the public authority intends to acquire private information.

2.12 It is therefore strongly recommended that a public authority consider an authorisation whenever the use or conduct of a CHIS is likely to engage an individual's rights under Article 8, whether this is through obtaining information, particularly private information, or simply through the covert manipulation of a relationship. An authorisation will be required if a relationship exists between the subject and the CHIS, even if specific information has not been sought by the public authority.

Establishing, maintaining and using a relationship

2.13 The word 'establishes' when applied to a relationship means 'set up'. It does not require, as 'maintains' does, endurance over any particular period. Consequently, a relationship of seller and buyer

may be deemed to exist between a shopkeeper and a customer even if only a single transaction takes place. Repetition is not always necessary to give rise to a relationship, but whether or not a relationship exists depends on all the circumstances including the length of time of the contact between seller and buyer and the nature of any covert activity.

Example 1: Intelligence suggests that a local shopkeeper is openly selling alcohol to underage customers, without any questions being asked. A juvenile is engaged and trained by a public authority and then deployed in order to make a purchase of alcohol. In these circumstances any relationship, if established at all, is likely to be so limited in regards to the requirements of the 2000 Act that a public authority may conclude that a CHIS authorisation is unnecessary. However, if the test purchaser is wearing recording equipment but is not authorised as a CHIS, consideration should be given to granting a directed surveillance authorisation.

Example 2: In similar circumstances, intelligence suggests that a shopkeeper will sell alcohol to juveniles from a room at the back of the shop, providing they have first got to know and trust them. As a consequence the public authority decides to deploy its operative on a number of occasions, to befriend the shopkeeper and gain their trust, in order to purchase alcohol. In these circumstances a relationship has been established and maintained for a covert purpose and therefore a CHIS authorisation should be obtained.

2.14 Any police officer deployed as a ‘relevant source’ in England and Wales will be required to comply with and uphold the principles and standards of professional behaviour set out in the College of Policing Code of Ethics.

Legend building

2.15 When a relevant source is deployed to establish their ‘legend’/ build up their cover profile, an authorisation must be sought under the 2000 Act if the activity will interfere with an individual’s Article 8

rights. The individual does not have to be the subject of a future investigation. Interference with any individual's Article 8 rights requires authorisation under the 2000 Act.

Human source activity falling outside CHIS definition

2.16 Not all human source activity will meet the definition of a CHIS. For example, a source may be a public volunteer who discloses information out of professional or statutory duty, or has been tasked to obtain information other than by way of a relationship.

Public volunteers

2.17 In many cases involving human sources, a relationship will not have been established or maintained for a covert purpose. Many sources merely volunteer or provide information that is within their personal knowledge, without being induced, asked, or tasked by a public authority. This means that the source is not a CHIS for the purposes of the 2000 Act and no authorisation under the 2000 Act is required.⁷

Example 1: A member of the public volunteers a piece of information to a member of a public authority regarding something they have witnessed in their neighbourhood. The member of the public would not be regarded as a CHIS. They are not passing information as a result of a relationship which has been established or maintained for a covert purpose.

⁷ See Chapter 2 of this code for further guidance on types of source activity to which authorisations under Part II of the 2000 Act may or may not apply.

Example 2: A caller to a confidential hotline (such as Crimestoppers, the Customs Hotline, the Anti-Terrorist Hotline, or the Security Service Public Telephone Number) reveals that they know of criminal or terrorist activity. Even if the caller is involved in the activities on which they are reporting, the caller would not be considered a CHIS as the information is not being disclosed on the basis of a relationship which was established or maintained for that covert purpose. However, should the caller be asked to maintain their relationship with those involved and to continue to supply information, an authorisation for the use or conduct of a CHIS may be appropriate.

Professional or statutory duty

2.18 Certain individuals will be required to provide information to public authorities or designated bodies out of professional or statutory duty. For example, employees within organisations regulated by the money laundering provisions of the Proceeds of Crime Act 2002 will be required to comply with the Money Laundering Regulations 2003 and report suspicious transactions. Similarly, financial officials, accountants or company administrators may have a duty to provide information that they have obtained by virtue of their position to the Serious Fraud Office.

2.19 Any such regulatory or professional disclosures should not result in these individuals meeting the definition of a CHIS, as the business or professional relationships from which the information derives will not have been established or maintained for the covert purpose of disclosing such information.

2.20 Furthermore, this reporting is undertaken 'in accordance with the law' and therefore any interference with an individual's privacy (Article 8 rights) will be in accordance with Article 8(2) ECHR.

2.21 This statutory or professional duty, however, would not extend to the situation where a person is asked to provide information which they acquire as a result of an existing professional or business relationship with the subject but that person is under no obligation to pass it on. For example, a travel agent who is asked by the police to

find out when a regular client next intends to fly to a particular destination is not under an obligation to pass this information on. In these circumstances a CHIS authorisation may be appropriate.

Tasking not involving relationships

2.22 Tasking a person to obtain information covertly may result in authorisation under Part II of the 2000 Act being appropriate. However, this will not be true in all circumstances. For example, where the tasking given to a person does not require that person to establish or maintain a relationship for the purpose of obtaining, providing access to or disclosing the information sought or where the information is already within the personal knowledge of the individual, that person will not be a CHIS.

Example: A member of the public is asked by a member of a public authority to maintain a record of all vehicles arriving and leaving a specific location or to record the details of visitors to a neighbouring house. A relationship has not been established or maintained in order to gather the information and a CHIS authorisation is therefore not available. Other authorisations under the Act (for example, directed surveillance) may need to be considered where there is an interference with the Article 8 rights of an individual.

Identifying when a human source becomes a CHIS

2.23 Individuals or members of organisations (e.g. travel agents, housing associations and taxi companies) who, because of their work or role have access to personal information, may voluntarily provide information to the police on a repeated basis and need to be managed appropriately. Public authorities must keep such human sources under constant review to ensure that they are managed with an appropriate level of sensitivity and confidentiality, and to establish whether, at any given stage, they should be authorised as a CHIS.

2.24 Determining the status of an individual or organisation is a matter of judgement by the public authority. Public authorities should avoid inducing individuals to engage in the conduct of a CHIS either expressly or implicitly without obtaining a CHIS authorisation.

Example 2: Mr Y volunteers information to a member of a public authority about a work colleague out of civic duty. Mr Y is not a CHIS at this stage as he has not established or maintained (or been asked to establish or maintain) a relationship with his colleague for the covert purpose of obtaining and disclosing information. However, Mr Y is subsequently contacted by the public authority and is asked if he would ascertain certain specific information about his colleague. At this point, it is likely that Mr Y's relationship with his colleague is being maintained and used for the covert purpose of providing that information. A CHIS authorisation would therefore be appropriate to authorise interference with the Article 8 right to respect for private and family life of Mr Y's work colleague.

2.25 However, the tasking of a person should not be used as the sole benchmark in seeking a CHIS authorisation. It is the activity of the CHIS in exploiting a relationship for a covert purpose which is ultimately authorised by the 2000 Act, whether or not that CHIS is asked to do so by a public authority. It is possible therefore that a person will become engaged in the conduct of a CHIS without a public authority inducing, asking or assisting the person to engage in that conduct.

Chapter 3

GENERAL RULES ON AUTHORISATIONS

Authorising officer

3.1 Responsibility for giving the authorisation will depend on which public authority is responsible for the CHIS. For the purposes of this and future chapters, the person in a public authority responsible for granting an authorisation will be referred to as the ‘authorising officer’. The relevant public authorities and authorising officers are listed in the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 as amended by the Regulation of Investigatory Powers (Covert Human Intelligence Sources: Relevant Sources) Order 2013.

Necessity and proportionality

3.2 The 2000 Act stipulates that the authorising officer must believe that an authorisation for the use or conduct of a CHIS is necessary in the circumstances of the particular case for one or more of the statutory grounds listed in section 29(3) of the 2000 Act.

3.3 If the use or conduct of the CHIS is deemed necessary, on one or more of the statutory grounds, the person granting the authorisation must also believe that it is proportionate to what is sought to be achieved by carrying it out. This involves balancing the seriousness of the intrusion into the private or family life of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.

3.4 The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence

may be serious will not alone render the use or conduct of a CHIS proportionate. Similarly, an offence may be so minor that any deployment of a CHIS would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

3.5 The following elements of proportionality should therefore be considered:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

Extent of authorisations

3.6 An authorisation under Part II of the 2000 Act for the use or conduct of a CHIS will provide lawful authority for any such activity that:

- involves the use or conduct of a CHIS as is specified or described in the authorisation;
- is carried out by or in relation to the person to whose actions as a CHIS the authorisation relates; and
- is carried out for the purposes of, or in connection with, the investigation or operation so described.⁸

3.7 In the above context, it is important that the CHIS is fully aware of the extent and limits of any conduct authorised and that those involved in the use of a CHIS are fully aware of the extent and limits of the authorisation in question.

⁸ See section 29(4) of the 2000 Act.

Collateral intrusion

3.8 Before authorising the use or conduct of a source, the authorising officer should take into account the risk of interference with the private and family life of persons who are not the intended subjects of the CHIS activity (collateral intrusion).

3.9 Measures should be taken, wherever practicable, to avoid or minimize interference with the private and family life of those who are not the intended subjects of the CHIS activity. Where such collateral intrusion is unavoidable, the activities may still be authorised providing this collateral intrusion is considered proportionate to the aims of the intended intrusion. Any collateral intrusion should be kept to the minimum necessary to achieve the objective of the operation.

3.10 All applications should therefore include an assessment of the risk of any collateral intrusion, and details of any measures taken to limit this, to enable the authorising officer fully to consider the proportionality of the proposed use or conduct of a CHIS.

3.11 Where CHIS activity is deliberately proposed against individuals who are not suspected of direct or culpable involvement in the matter being investigated, interference with the private and family life of such individuals should not be considered as collateral intrusion but rather as intended intrusion. Any such interference should be carefully considered against the necessity and proportionality criteria as described above.

Example 1: A relevant source is deployed to obtain information about the activities of a suspected criminal gang under CHIS authorisation. It is assessed that the relevant source will in the course of this deployment obtain private information about some individuals who are not involved in criminal activities and are of no interest to the investigation. The authorising officer should consider the proportionality of this collateral intrusion, and whether sufficient measures are to be taken to limit it, when granting the authorisation.

Example 2: The police seek to establish the whereabouts of Mr W in the interests of national security. In order to do so, a relevant source is deployed to seek to obtain this information from Mr P, an associate of Mr W who is not of direct security interest. An application for a CHIS authorisation is made to authorise the deployment. The authorising officer will need to consider the necessity and proportionality of the operation against Mr P and Mr W, who will be the direct subjects of the intrusion. The authorising officer will also need to consider the proportionality of any collateral intrusion that will arise if there is any additional interference with the private and family life of other individuals of no interest to the investigation.

Reviewing and renewing authorisations

3.12 Except where enhanced arrangements under the 2013 Order apply, the authorising officer who grants an authorisation should, where possible, be responsible for considering subsequent renewals of that authorisation and any related security and welfare issues.

3.13 The authorising officer will stipulate the frequency of formal reviews and the controller (see paragraph 6.9 below) should maintain an audit of case work sufficient to ensure that the use or conduct of the CHIS remains within the parameters of the extant authorisation. This will not prevent additional reviews being conducted by the authorising officer in response to changing circumstances such as described below.

3.14 Where the nature or extent of intrusion into the private or family life of any person becomes greater than that anticipated in the original authorisation, the authorising officer should immediately review the authorisation and reconsider the proportionality of the operation. This should be highlighted at the next renewal.

3.15 Where a CHIS authorisation provides for interference with the private and family life of initially unidentified individuals whose identity is later established, a new authorisation is not required provided the scope of the original authorisation envisaged interference with the private and family life of such individuals.

Example: An authorisation is obtained by the police to authorise a CHIS to use her relationship with ‘Mr X and his close associates’ for the covert purpose of providing information relating to their suspected involvement in a crime. Mr X introduces the CHIS to Mr A, a close associate of Mr X. It is assessed that obtaining more information on Mr A will assist the investigation. The CHIS may use her relationship with Mr A to obtain such information but the review of the authorisation should specify any interference with the private and family life of ‘Mr X and his associates, including Mr A’ and that such an interference is in accordance with the original authorisation.

3.16 Any proposed changes to the *nature* of the CHIS operation (i.e. the activities involved) should immediately be brought to the attention of the authorising officer. The authorising officer should consider whether the proposed changes are within the scope of the existing authorisation and whether they are proportionate (bearing in mind any extra interference with private or family life or collateral intrusion), before approving or rejecting them. Any such changes should be highlighted at the next renewal.

Local considerations and community impact assessments

3.17 Any person granting or applying for an authorisation will also need to be aware of any particular sensitivities in the local community where the CHIS is being used and of similar activities being undertaken by other public authorities which could have an impact on the deployment of the CHIS. Consideration should also be given to any adverse impact on community confidence or safety that may result from the use or conduct of a CHIS or use of information obtained from that CHIS.

3.18 It is therefore recommended that where an authorising officer from a public authority considers that conflicts might arise they should, where possible, consult a senior officer within the police force area in which the CHIS is deployed. All public authorities, where possible, should consider consulting with other relevant public authorities to gauge community impact.

Combined authorisations

3.19 A single authorisation may combine two or more different authorisations under Part II of the 2000 Act.⁹ For example, a single authorisation may combine authorisations for intrusive surveillance and the conduct of a CHIS. In such cases the provisions applicable to each of the authorisations must be considered separately by the appropriate authorising officer. Thus, a superintendent or an assistant chief constable (for relevant sources), can authorise the conduct of a CHIS but an authorisation for intrusive surveillance by the police needs the separate authorisation of a chief constable (and the prior approval of a Surveillance Commissioner, except in cases of urgency).

3.20 Where an authorisation for the use or conduct of a CHIS is combined with a Secretary of State authorisation for intrusive surveillance, the combined authorisation must be issued by the Secretary of State.

3.21 The above considerations do not preclude public authorities from obtaining separate authorisations.

Operations involving multiple CHIS

3.22 A single authorisation under Part II of the 2000 Act may be used to authorise more than one CHIS. However, this is only likely to be appropriate for operations involving the conduct of several undercover operatives acting as CHISs in situations where the activities to be authorised, the subjects of the operation, the interference with private and family life, the likely collateral intrusion and the environmental or operational risk assessments are the same for each officer. If an authorisation includes more than one relevant

⁹ See section 43(2) of the 2000 Act.

source, each relevant source must be clearly identifiable within the documentation sent to the OSC. In these circumstances adequate records must be kept of the length of deployment of a relevant source to ensure the enhanced authorisation process set out in the 2013 Order and Annex B of this code can be adhered to.

Covert surveillance of a potential CHIS

3.23 It may be necessary to deploy covert surveillance against a potential CHIS, other than those acting in the capacity of an undercover operative, as part of the process of assessing their suitability for recruitment, or in planning how best to make the approach to them. Covert surveillance in such circumstances may or may not be necessary on one of the statutory grounds on which directed surveillance authorisations can be granted, depending on the facts of the case. Whether or not a directed surveillance authorisation is available, any such surveillance must be justifiable under Article 8(2) of the ECHR.

Use of covert human intelligence sources with technical equipment

3.24 A CHIS wearing or carrying a surveillance device does not need a separate intrusive or directed surveillance authorisation, provided the device will only be used in the presence of the CHIS. However, if a surveillance device is to be used other than in the presence of the CHIS, an intrusive or directed surveillance authorisation should be obtained where appropriate, together with an authorisation for interference with property, if applicable. See the Covert Surveillance and Property Interference Code of Practice.

3.25 A CHIS, whether or not wearing or carrying a surveillance device, in residential premises or a private vehicle, does not require additional authorisation to record any activity taking place inside those premises or that vehicle which takes place in their presence. This also applies to the recording of telephone conversations or other forms of communication, other than by interception, which takes place in the source's presence. Authorisation for the use or conduct of that source may be obtained in the usual way.

Use of covert human intelligence sources by local authorities

3.26 The Protection of Freedoms Act 2012 amended the 2000 Act to make local authority authorisation of a CHIS subject to judicial approval. The change means that local authorities need to obtain an order approving the grant or renewal of an authorisation from a Justice of the Peace before it can take effect. If the JP is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate they will issue an order approving the grant or renewal for the use of the technique as described in the application. The amendment means that local authorities are no longer able to orally authorise the use of RIPA techniques. The detail of these changes is set out in detail in separate guidance for local authorities and the judiciary. This guidance is available on the .gov.uk website. In Scotland this requirement only applies to authorisations for communications data as the use of the other techniques is governed by RIP(S)A. In Northern Ireland this requirement only applies to authorisations where the grant or renewal relates to a Northern Ireland excepted or reserved matter. Where such an authorisation is required by a local authority in Northern Ireland, an application for a grant or renewal should be made to a district judge. For other authorisations, local authorities in Northern Ireland should refer to the general requirements for authorisation set out in this code.

3.27 Elected members of a local authority should review the authority's use of the 2000 Act and set the policy at least once a year. They should also consider internal reports on use of the 2000 Act on a regular basis to ensure that it is being used consistently with the local authority's policy and that the policy remains fit for purpose.

Chapter 4

SPECIAL CONSIDERATIONS FOR AUTHORISATIONS

Legally privileged material and other confidential information

4.1 The 2000 Act does not provide any special protection for ‘confidential information’. Nevertheless, particular care should be taken in cases where the subject of the intrusion might reasonably expect a high degree of privacy, or where confidential information is involved. Confidential information consists of matters subject to legal privilege, confidential personal information, confidential constituent information or confidential journalistic material. So, for example, extra care should be taken where, through the use or conduct of a CHIS, it would be possible to acquire knowledge of discussions between a minister of religion and an individual relating to the latter’s spiritual welfare, or between a Member of Parliament and the individual or group where they are constituents relating to private constituency matters, or wherever matters of medical or journalistic confidentiality or legal privilege may be involved. References to a Member of Parliament include references to Members of both Houses of the UK Parliament, the European Parliament, the Scottish Parliament, the Welsh Assembly and the Northern Ireland Assembly.

4.2 In cases where through the use or conduct of a CHIS it is likely that knowledge of legally privileged material or other confidential information will be acquired, the deployment of the CHIS is subject to a higher level of authorisation. The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 lists the authorising officer for each public authority permitted to authorise such use or conduct of a CHIS.

4.3 There may be circumstances when a ‘relevant source’ as described in the 2013 Order will have access to legally privileged or confidential information. In such circumstances, the authorisation processes set out in the 2010 Order and the 2013 Order should be adhered to. The authorisation levels for access to confidential material are set out at Annex A.

Matters subject to legal privilege – introduction

4.4 Section 98 of the 1997 Act defines those matters that are subject to legal privilege. Under this definition, legal privilege does not apply to communications or items held, or oral communications made, with the intention of furthering a criminal purpose (whether the lawyer is acting unwittingly or culpably). Legally privileged communications will lose their protection if the professional legal adviser is intending to hold or use them for a criminal purpose. But privilege is not lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence.

4.5 Public authorities may obtain knowledge of matters subject to legal privilege via CHIS in three scenarios: first, where the public authority responsible for the CHIS deliberately authorised the use or conduct of the CHIS in order to obtain knowledge of matters subject to legal privilege; second, where the CHIS obtains knowledge of matters subject to legal privilege through conduct incidental (within the meaning of section 26(7)(a)) to their conduct as a CHIS; and, third, where a CHIS obtains knowledge of matters subject to legal privilege where their conduct cannot properly be regarded as incidental to their conduct as a CHIS. Separate guidance is relevant to each scenario.

Authorisations for the use or conduct of a CHIS to obtain, provide access to or disclose knowledge of matters subject to legal privilege

4.6 If a public authority seeks to grant or renew an authorisation for the use or conduct of a CHIS in order to obtain, provide access to or disclose knowledge of matters subject to legal privilege, the 2010

Order will apply. The 2010 Order creates an enhanced regime of prior approval for such authorisations. The 2010 Order provides that before an authorising officer grants or renews an authorisation to which the Order applies, they must give notice to the relevant approving officer. The relevant approving officer will be the Secretary of State in the case of a member of the intelligence services, an official of the Ministry of Defence, an individual holding an office, rank or position in Her Majesty's Prison Service or the Northern Ireland Prison Service. In all other cases, the relevant approving officer will be an ordinary Surveillance Commissioner. The authorising officer is prohibited from granting or renewing an authorisation to which the 2010 Order applies until they have received confirmation in writing that the approving officer has approved the application. If the approving officer does not approve the application, the authorising officer may still grant an authorisation in respect of the use or conduct of the CHIS in question, but may not authorise the use or conduct of the CHIS to obtain, provide access to or disclose knowledge of matters subject to legal privilege.

4.7 Approving officers may only approve, and authorising officers may only authorise, the use or conduct of CHIS to acquire knowledge of matters subject to legal privilege if they are satisfied that there are exceptional and compelling circumstances that make the authorisation necessary. Such circumstances will arise only in a very restricted range of cases, such as where there is a threat to life or limb, or to national security, and the use or conduct of a CHIS to acquire knowledge of matters subject to legal privilege is reasonably regarded as likely to yield intelligence necessary to counter the threat.

Circumstances in which the obtaining of knowledge of matters subject to legal privilege by a CHIS or public authority is incidental to the conduct authorised in the authorisation

4.8 The reactive nature of the work of a CHIS, and the need for a CHIS to maintain cover, may make it necessary for a CHIS to engage in conduct which was not envisaged at the time the authorisation was granted, but which is incidental to that conduct.

Such incidental conduct is regarded as properly authorised by virtue of sections 26(7)(a), 27 and 29(4) of the 2000 Act, even though it was not specified in the initial authorisation.

4.9 This is likely to occur only in exceptional circumstances, such as where the obtaining of such knowledge is necessary to protect life and limb, including in relation to the CHIS, or national security, in circumstances that were not envisaged at the time the authorisation was granted.

4.10 If any of these situations arise, the public authority should draw it to the attention of the relevant Commissioner or Inspector during the next inspection (at which the material should be made available if requested). In addition, the public authority in question should ensure that any knowledge of matters subject to legal privilege obtained through conduct incidental to the use or conduct of a CHIS specified in the authorisation is not used in law enforcement investigations or criminal prosecutions.

4.11 If it becomes apparent that it will be necessary for the CHIS to continue to obtain, provide access to or disclose knowledge of matters subject to legal privilege, the initial authorisation should be replaced by an authorisation that has been subject to the prior approval procedure set out in the 2010 Order at the earliest reasonable opportunity.

Unintentional obtaining of knowledge of matters subject to legal privilege by a CHIS

4.12 Public authorities should make every effort to avoid their CHIS unintentionally obtaining, providing access to or disclosing knowledge of matters subject to legal privilege. If a public authority assesses that a CHIS may be exposed to such knowledge unintentionally, the public authority should task the CHIS in such a way that this possibility is reduced as far as possible. When debriefing the CHIS, the public authority should make every effort to ensure that any knowledge of matters subject to legal privilege which the CHIS may have obtained is not disclosed to the public authority, unless there are exceptional and compelling circumstances that make such disclosure necessary. If, despite these steps, knowledge of

matters subject to legal privilege is unintentionally disclosed to the public authority, the public authority in question should ensure that it is not used in law enforcement investigations or criminal prosecutions. Any unintentional obtaining of knowledge of matters subject to legal privilege by a public authority, together with a description of all steps taken in relation to that material, should be drawn to the attention of the relevant Commissioner or Inspector during the next inspection (at which the material should be made available if requested).

The use and handling of material subject to legal privilege

4.13 Legally privileged information is particularly sensitive and any use or conduct of CHIS which obtains, provides access to or discloses such material may give rise to issues under Article 6 of the ECHR (right to a fair trial) as well as engaging Article 8.

4.14 Where public authorities deliberately obtain knowledge of matters subject to legal privilege via the conduct of a CHIS, they may use it to counter the threat which led them to obtain it; but not for other purposes. In particular, public authorities should ensure that knowledge of matters subject to legal privilege is kept separate from law enforcement investigations or criminal prosecutions.

4.15 In cases likely to result in the obtaining by a public authority of knowledge of matters subject to legal privilege, the authorising officer or Surveillance Commissioner may require regular reporting so as to be able to decide whether the authorisation should continue. In those cases where knowledge of matters subject to legal privilege has been obtained and retained, the matter should be reported to the authorising officer by means of a review and to the relevant Commissioner or Inspector during the next inspection (at which the material should be made available if requested).

4.16 A substantial proportion of the communications between a lawyer and their client(s) may be subject to legal privilege. Therefore, in any case where a lawyer is the subject of an investigation or operation, authorising officers should consider whether the special

safeguards outlined in this chapter apply. Any material which has been retained from any such investigation or operation should be notified to the relevant Commissioner or Inspector during their next inspection and made available on request.

4.17 Where there is any doubt as to the handling and dissemination of information which may be subject to legal privilege, advice should be sought from a legal adviser within the relevant public authority before any further dissemination of the material takes place. Similar advice should also be sought where there is doubt over whether information is not subject to legal privilege due to the ‘in furtherance of a criminal purpose’ exception. The retention of legally privileged information, or its dissemination to an outside body, should be accompanied by a clear warning that it is subject to legal privilege. It should be safeguarded by taking reasonable steps to ensure there is no possibility of it becoming available, or its contents becoming known, to any person whose possession of it might prejudice any criminal or civil proceedings to which the information relates. Any dissemination of legally privileged material to an outside body should be notified to the relevant Commissioner or Inspector during their next inspection.

Confidential information

4.18 Similar consideration must also be given to authorisations for use or conduct that are likely to result in the obtaining of confidential personal information, confidential constituent information and confidential journalistic material. Where such material has been acquired and retained, the matter should be reported to the relevant Commissioner or Inspector during their next inspection and the material be made available to him if requested.

4.19 Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling of a person (whether living or dead) who can be identified from it.¹⁰ Such information, which can include both oral

¹⁰ **Spiritual counselling** means conversations between a person and a religious authority acting in an official capacity, where the individual being counselled is seeking or the religious authority is imparting forgiveness, absolution or the resolution of conscience in accordance with their faith.

and written communications, is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. Examples might include consultations between a health professional and a patient, or information from a patient's medical records.

4.20 Confidential constituent information is information held in confidence in relation to communications between a Member of Parliament and a constituent in respect of constituency matters. Again, such information is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation.

4.21 Confidential journalistic material includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking.

4.22 Where there is any doubt as to the handling and dissemination of confidential information, advice should be sought from a legal adviser, who is independent from the investigation, within the relevant public authority before any further dissemination of the material takes place. Any dissemination of confidential material to an outside body should be notified to the relevant Commissioner or Inspector during their next inspection.

Vulnerable individuals

4.23 A vulnerable individual is a person who by reason of mental disorder or vulnerability, other disability, age or illness, is or may be unable to take care of themselves, or unable to protect themselves against significant harm or exploitation. Where it is known or suspected that an individual may be vulnerable, they should only be authorised to act as a CHIS in the most exceptional circumstances. In these cases, Annex A lists the authorising officer for each public authority permitted to authorise the use of a vulnerable individual as a CHIS.

Juvenile sources

4.24 Special safeguards also apply to the use or conduct of juveniles, that is, those under 18 years old, as sources. On no occasion should the use or conduct of a CHIS under 16 years of age be authorised to give information against their parents or any person who has parental responsibility for them. In other cases, authorisations should not be granted unless the special provisions contained within The Regulation of Investigatory Powers (Juveniles) Order 2000; SI No. 2793 are satisfied. Authorisations for juvenile sources should be granted by those listed in the attached table at Annex A. The duration of such an authorisation is one month from the time of grant or renewal (instead of 12 months). For the purpose of these rules, the age test is applied at the time of the grant or renewal of the authorisation.

Scotland

4.25 Where all the conduct authorised is likely to take place in Scotland, authorisations should be granted under RIP(S)A, unless:

- the authorisation is being obtained by those public authorities listed in section 46(3) of the 2000 Act and the Regulation of Investigatory Powers (Authorisations Extending to Scotland) Order 2000; SI No. 2418;
- the authorisation is to be granted or renewed (by any relevant public authority) for the purposes of national security or the economic well-being of the UK; or
- the authorisation authorises conduct that is surveillance by virtue of section 48(4) of the 2000 Act.

4.26 This code of practice is extended to Scotland in relation to authorisations granted under Part II of the 2000 Act which apply to Scotland. A separate code of practice applies in relation to authorisations granted under RIP(S)A.

International

4.27 Authorisations under the 2000 Act can be given for the use or conduct of CHIS both inside and outside the UK. However, authorisations for actions outside the UK can usually only validate them for the purposes of UK law.

4.28 Public authorities are therefore advised to seek authorisations where available under the 2000 Act for any overseas operations where the subject of investigation is a UK national or is likely to become the subject of criminal or civil proceedings in the UK, or if the operation is likely to affect a UK national or give rise to material likely to be used in evidence before a UK court.

4.29 Public authorities must have in place internal systems to manage any overseas CHIS deployments and it is recognised practice for UK law enforcement agencies to follow the authorisation and management regime under the 2000 Act, even where such deployments are only intended to impact locally and are therefore authorised under domestic law. However, public authorities should take care to monitor such deployments to identify where civil or criminal proceedings may become a prospect in the UK and ensure that, where appropriate, an authorisation under Part II of the 2000 Act is sought if this becomes the case.

4.30 The Human Rights Act 1998 applies to all activity taking place within the UK. This should be taken to include overseas territories and facilities which are within the jurisdiction of the UK. Authorisations under the 2000 Act may therefore be appropriate for overseas covert operations occurring in UK Embassies, military bases, detention facilities, etc., in order to comply with rights to privacy under Article 8 of the ECHR.¹¹

4.31 Members of foreign law enforcement or other agencies or CHIS of those agencies may be authorised under the 2000 Act in the UK in support of domestic and international investigations. When a member of a foreign law enforcement agency is authorised in support of a domestic or international investigation or operation consideration

¹¹ See *R v Al Skeini* June 2007. If conduct is to take place overseas the ACPO Covert Investigation (Legislation and Guidance) Steering Group may be able to offer additional advice.

should be given to authorising the individual at the level prescribed by the 2013 Order as if the individual holds an ‘office, rank or position’ with an organisation listed in the same order.

Online covert activity

4.32 The use of the internet may be required to gather information prior to and/or during a CHIS operation, which may amount to directed surveillance. Alternatively the CHIS may need to communicate online, for example this may involve contacting individuals using social media websites. Whenever a public authority intends to use the internet as part of an investigation, they must first consider whether the proposed activity is likely to interfere with a person’s Article 8 rights, including the effect of any collateral intrusion. Any activity likely to interfere with an individual’s Article 8 rights should only be used when necessary and proportionate to meet the objectives of a specific case. Where it is considered that private information is likely to be obtained, an authorisation (combined or separate) must be sought as set out elsewhere in this code.

Chapter 5

AUTHORISATION PROCEDURES FOR COVERT HUMAN INTELLIGENCE SOURCES

Authorisation criteria

5.1 Under section 29(3) of the 2000 Act an authorisation for the use or conduct of a CHIS may be granted by the authorising officer where they believe that the authorisation is necessary:

- in the interests of national security;¹²
- for the purpose of preventing or detecting¹³ crime or of preventing disorder;
- in the interests of the economic well-being of the UK;
- in the interests of public safety;
- for the purpose of protecting public health;¹⁴
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; or for any other purpose prescribed in an order made by the Secretary of State.¹⁵

12 One of the functions of the Security Service is the protection of national security and in particular the protection against threats from terrorism. These functions extend throughout the UK. An authorising officer in another public authority should not issue an authorisation under Part II of the 2000 Act where the operation or investigation falls within the responsibilities of the Security Service, as set out above, except where it is to be carried out by a Special Branch, Counter Terrorism Unit or Counter Terrorism Intelligence Unit or where the Security Service has agreed that another public authority can authorise the use or conduct of a CHIS which would normally fall within the responsibilities of the Security Service. HM Forces may also undertake operations in connection with national security in support of the Security Service or other Civil Powers.

13 Detecting crime is defined in section 81(5) of the 2000 Act. Preventing and detecting crime goes beyond the prosecution of offenders and includes actions taken to avert, end or disrupt the commission of criminal offences.

14 This could include investigations into infectious diseases, contaminated products or the illicit sale of pharmaceuticals.

15 This could only be for a purpose which satisfies the criteria set out in Article 8(2) of the ECHR.

5.2 The authorising officer must also believe that the authorised use or conduct of CHIS is proportionate to what is sought to be achieved by that use or conduct.

Relevant public authorities

5.3 The public authorities entitled to authorise the use or conduct of a CHIS, together with the specific purposes for which each public authority may authorise the use or conduct of a CHIS, are laid out in Schedule 1 of the 2000 Act and the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 as amended by the 2013 Order.

Authorisation procedures

5.4 Responsibility for authorising the use or conduct of a CHIS rests with the authorising officer and all authorisations require the personal authority of the authorising officer. The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 as amended by the 2013 Order designate the authorising officer for each different public authority and the officers entitled to act only in urgent cases. In certain circumstances the Secretary of State will be the authorising officer (see section 30(2) of the 2000 Act).

5.5 The authorising officer must give authorisations in writing, except in urgent cases, where they may be given orally. In such cases, a statement that the authorising officer has expressly authorised the action should be recorded in writing by the applicant (or the person with whom the authorising officer spoke) as a priority. This statement need not contain the full detail of the application, which should however subsequently be recorded in writing when reasonably practicable (generally the next working day).

5.6 Other officers entitled to act in urgent cases may only give authorisation in writing e.g. written authorisation for directed surveillance given by an Inspector.

5.7 A case is not normally to be regarded as urgent unless the time that would elapse before the authorising officer was available to grant the authorisation would, in the judgement of the person giving the authorisation, be likely to endanger life or jeopardise the operation or investigation for which the authorisation was being given. An authorisation is not to be regarded as urgent where the need for an authorisation has been neglected or the urgency is of the applicant's or authorising officer's own making.

5.8 Authorising officers should not be responsible for authorising their own activities, e.g. those in which they, themselves, are to act as the CHIS or as the handler of the CHIS. Furthermore, authorising officers should, where possible, be independent of the investigation. However, it is recognised that this is not always possible, especially in the cases of small organisations, or where it is necessary to act urgently or for security reasons. Where an authorising officer authorises their own activity the central record of authorisations should highlight this and the attention of a Commissioner or Inspector should be invited to it during the next inspection.

5.9 Authorising officers within the Police Service of Scotland and the National Crime Agency (NCA) may only grant authorisations on application by a member of (including those formally seconded to) their own service or agency. The same rule applies to authorising officers within police forces, unless relevant Chief Officers have made collaboration agreements under the Police Act 1996. Authorising officers within Her Majesty's Revenue and Customs (HMRC) may only grant authorisations on application by an officer of Revenue and Customs.

5.10 All authorisations of relevant sources by public authorities named in the Regulation of Investigatory Powers (Covert Human Intelligence Sources: Relevant Sources) Order 2013 should be notified to the Office for the Surveillance Commissioners (OSC) when granted by the authorising officer, save where there is a requirement to seek prior approval. The authorisation should be notified to the OSC within seven days. A Commissioner may provide comments to the authorising officer. The Authorising Officer will be advised promptly of any comments made by a Commissioner. The

Authorising Officer will wish to consider all comments made by the Commissioners. Public Authorities listed in the 2013 Order should provide the OSC with the authorisation and associated risk assessment for each relevant source.

Information to be provided in applications for authorisation

5.11 An application for authorisation for the use or conduct of a CHIS should be in writing and record:

- the reasons why the authorisation is necessary in the particular case and on the grounds listed in section 29(3) of the 2000 Act (e.g. for the purpose of preventing or detecting crime);
- the purpose for which the CHIS will be tasked or deployed (e.g. in relation to drug supply, stolen property, a series of racially motivated crimes etc.);
- where a specific investigation or operation is involved, the nature of that investigation or operation;
- the nature of what the CHIS conduct will be;
- the details of any potential collateral intrusion and why the intrusion is justified;
- the details of any confidential information that is likely to be obtained as a consequence of the authorisation;
- the reasons why the authorisation is considered proportionate to what it seeks to achieve;
- the level of authorisation required (or recommended, where that is different); and
- a subsequent record of whether authorisation was given or refused, by whom and the time and date.

5.12 Additionally, in urgent cases, the authorisation should record (as the case may be):

- the reasons why the authorising officer considered the case so urgent that an oral instead of a written authorisation was given; or
- the reasons why the officer entitled to act in urgent cases considered the case so urgent and why it was not reasonably practicable for the application to be considered by the authorising officer.

5.13 Where the authorisation is oral, the detail referred to above should be recorded in writing by the applicant when reasonably practicable (generally the next working day).

Duration of authorisations

5.14 A written authorisation will, unless renewed, cease to have effect at the end of a period of 12 months beginning with the day on which it took effect, except in the case of juvenile CHIS.

5.15 Urgent oral authorisations or authorisations granted or renewed by a person who is entitled to act only in urgent cases will, unless renewed, cease to have effect after 72 hours, beginning with the time when the authorisation was granted. Local authorities are no longer able to orally authorise the use of RIPA techniques. Out-of-hours arrangements should be in place with HMCS to deal with out-of-hours applications.

Reviews

5.16 Regular reviews of authorisations should be undertaken by the authorising officer to assess whether it remains necessary and proportionate to use a CHIS and whether the authorisation remains justified. The review should include the use made of the CHIS during the period authorised; the tasks given to the CHIS; the information obtained from the CHIS; and the reasons why executive action is not possible at this stage. The results of a review should be retained for at least three years (see chapter 7). Particular attention is drawn to the need to review authorisations frequently where the use of a CHIS provides access to confidential information or involves significant collateral intrusion.

5.17 In each case the authorising officer within each public authority should determine how often a review should take place. This should be as frequently as is considered necessary and practicable, but should not prevent reviews being conducted in response to changing circumstances.

Renewals

5.18 Before an authorising officer renews an authorisation, they must be satisfied that a review has been carried out of the use of a CHIS, as outlined above, and that the results of the review have been considered.

5.19 If, before an authorisation would cease to have effect, the authorising officer considers it necessary for the authorisation to continue for the purpose for which it was given, they may renew it in writing for a further period of 12 months. Renewals may also be granted orally in urgent cases and last for a period of 72 hours.

5.20 A renewal takes effect at the time at which the authorisation would have ceased to have effect but for the renewal. An application for renewal should therefore not be made until shortly before the authorisation period is drawing to an end.

5.21 Except where enhanced arrangements exist, the authorising officer who granted the authorisation, or the officer undertaking that function, should renew the authorisation. In the case of a relevant source, renewals for deployment beyond 12 months should be carried out by a Chief Constable or equivalent and pre-approved at a Surveillance Commissioner.

5.22 Authorisations may be renewed more than once, if necessary, provided they continue to meet the criteria for authorisation. Documentation of the renewal should be retained for at least three years (see Chapter 7).

5.23 All applications by public authorities named in the 2013 Order for an authorisation of a relevant source beyond 12 months (i.e. long-term authorisation) must be approved by an ordinary Surveillance Commissioner before authorisation by the appropriate authorising officer. The 2013 Order creates an enhanced regime of prior approval for such authorisations.

5.24 The 2013 Order defines long-term authorisation by reference to the cumulative periods for which the relevant source will be/has been authorised on the same investigation or operation. These must exceed 12 months (or where the 2010 Order applies, three months). If a

relevant source has not been authorised on the same investigation or operation for at least three years, any previous authorisations will be disregarded for the purposes of calculating the 12 months.

5.25 When deciding if the relevant source is authorised as part of the ‘same investigation or operation’ in calculating the period of total or accrued deployment or cumulative authorisation periods, the following should be considered:

- common subject or subjects of the investigation or operation;
- the nature and details of relationships established in previous or corresponding relevant investigations or operations;
- whether or not the current investigation is a development of or recommencement to previous periods of authorisation, which may include a focus on the same crime group or individuals;
- previous legend building activity by the relevant source that has a bearing by way of subject, locality, environment or other consistent factors should be considered in calculating the period; and
- the career history of the ‘relevant source’.

5.26 Public authorities named in the 2013 Order should notify the OSC at the nine-month point of any authorisation that may require renewal beyond 12 months (as calculated in the paragraph above).

Example 1: A 12-month authorisation has been granted by the Assistant Chief Constable of a police force for a relevant source against a subject for the purposes of collecting intelligence about drug supply. The authority is cancelled after six months because the subject disappears and there is insufficient evidence obtained at that time to prosecute. A year later the subject then returns to deal drugs in the area again and the police force wishes to authorise another relevant source against the subject. If the same relevant source is used, authorisation by an Assistant Chief Constable will be for maximum of six months. If the police force decides to use different relevant sources against the subject an Assistant Chief Constable can grant the authority for 12 months and it is treated as a new authority, provided the relevant sources have not been previously authorised in respect of the same investigation or operation.

Example 2: An authorisation for use of a relevant source is initially granted by an Assistant Chief Constable. After three months, it is apparent that legally privileged material may be accessed. Prior approval by the OSC was granted and a new authorisation granted by the Chief Constable for an additional three months. At the end of this period it was agreed the relevant source would no longer be likely to access any legally privileged material. A new authorisation for a maximum of six months could then be granted by the Assistant Chief Constable. The entire period of deployment, including the three months at the higher level for access to legally privileged material, would count toward the 12-month period. Who granted the authorisation for the relevant source and what type of material they had access to is not relevant for the purposes of calculating the 12-month period. If the authorisation is renewed at the end of the six-month period, it becomes a long-term authorisation and approval of the OSC and authorisation by the Chief Constable is required.

5.27 All applications for the renewal of an authorisation should record:

- whether this is the first renewal or every occasion on which the authorisation has been renewed previously;
- any significant changes to the information in the initial application;
- the reasons why it is necessary for the authorisation to continue;
- the use made of the CHIS in the period since the grant or, as the case may be, latest renewal of the authorisation;
- the tasks given to the CHIS during that period and the information obtained from the use or conduct of the CHIS; and
- the results of regular reviews of the use of the CHIS.

Cancellations

5.28 The authorising officer who granted or renewed the authorisation must cancel it if they are satisfied that the use or conduct of the CHIS no longer satisfies the criteria for authorisation or that arrangements for the CHIS's case no longer satisfy the requirements described in section 29 of the 2000 Act. Where the

authorising officer is no longer available, this duty will fall on the person who has taken over the role of authorising officer or the person who is acting as authorising officer.

5.29 Where necessary, the safety and welfare of the CHIS should continue to be taken into account after the authorisation has been cancelled. The AO will wish to satisfy themselves that all welfare matters are addressed.

Refusal of approval of long-term authorisation

5.30 If an Ordinary Surveillance Commissioner does not conclude a long-term authorisation should be granted by the Chief Constable (or equivalent), the relevant public authority may appeal against the decision to the Chief Surveillance Commissioner within seven days.

5.31 Any risk assessment produced for a relevant source should include details of how the relevant source can be safely extracted should approval by a Surveillance Commissioner be refused.

Chapter 6

MANAGEMENT OF COVERT HUMAN INTELLIGENCE SOURCES

Tasking

6.1 Tasking is the assignment given to the CHIS by the persons defined at sections 29(5)(a) and (b) of the 2000 Act, asking him to obtain, provide access to or disclose information. Authorisation for the use or conduct of a CHIS will be appropriate prior to any tasking where such tasking involves the CHIS establishing or maintaining a personal or other relationship for a covert purpose.

6.2 Authorisations should not be drawn so narrowly that a separate authorisation is required each time the CHIS is tasked. Rather, an authorisation might cover, in broad terms, the nature of the source's task. If the nature of the task changes significantly, then a new authorisation may need to be sought.

6.3 It is difficult to predict exactly what might occur each time a meeting with a CHIS takes place, or the CHIS meets the subject of an investigation. There may be occasions when unforeseen action or undertakings occur. When this happens, the occurrence must be recorded as soon as practicable after the event and if the existing authorisation is insufficient it should either be updated at a review (for minor amendments only) or it should be cancelled and a new authorisation should be obtained before any further such action is carried out.

6.4 Similarly, where it is intended to task a CHIS in a significantly greater or different way than previously identified, the persons defined at section 29(5)(a) or (b) of the 2000 Act must refer the proposed tasking to the authorising officer, who should consider whether the existing authorisation is sufficient or needs to be replaced. This should be done in advance of any tasking and the

details of such referrals must be recorded. Efforts should be made to minimise the number of authorisations per CHIS to the minimum necessary in order to avoid generating excessive paperwork.

Handlers and controllers

6.5 Public authorities should ensure that arrangements are in place for the proper oversight and management of CHIS, including appointing individual officers as defined in sections 29(4A) and (4B) and 29(5)(a) and (b) of the 2000 Act for each CHIS.

6.6 Oversight and management arrangements for undercover operatives, while following the principles of the Act, will differ, in order to reflect the specific role of such individuals as members of public authorities. The role of the handler will be undertaken by a person referred to as a ‘cover officer’ and the role of controller will be undertaken by a ‘covert operations manager’.

6.7 The person referred to in section 29(5)(a) of the 2000 Act (the ‘handler’) will have day-to-day responsibility for:

- dealing with the CHIS on behalf of the authority concerned;
- directing the day-to-day activities of the CHIS;
- recording the information supplied by the CHIS; and
- monitoring the CHIS’s security and welfare.

6.8 The handler of a CHIS will usually be of a rank or position below that of the authorising officer.

6.9 The person referred to in section 29(5)(b) of the 2000 Act (the ‘controller’) will normally be responsible for the management and supervision of the ‘handler’ and general oversight of the use of the CHIS.

Joint working

6.10 In cases where the authorisation is for the use or conduct of a CHIS whose activities benefit more than a single public authority, responsibilities for the management and oversight of that CHIS may be taken up by one authority or can be split between the authorities. The controller and handler of a CHIS need not be from the same public authority.

6.11 There are many cases where the activities of a CHIS may provide benefit to more than a single public authority. Such cases may include:

- the prevention or detection of criminal matters affecting a national or regional area, for example where the CHIS provides information relating to cross-boundary or international drug trafficking;
- the prevention or detection of criminal matters affecting crime and disorder, requiring joint agency operational activity, for example where a CHIS provides information relating to environmental health issues and offences of criminal damage, in a joint police/local authority anti-social behaviour operation on a housing estate; or
- matters of national security, for example where the CHIS provides information relating to terrorist activity and associated criminal offences for the benefit of the police and the Security Service.

6.12 In such situations, however, the public authorities involved must lay out in writing their agreed oversight arrangements.

6.13 Management responsibility for CHIS, and relevant roles, may also be divided between different police forces where the Chief Officers of the forces concerned have made a collaboration agreement under the Police Act 1996 and the collaboration agreement provides for this to happen.

Security and welfare

6.14 Any public authority deploying a CHIS should take into account the safety and welfare of that CHIS when carrying out actions in relation to an authorisation or tasking, and the foreseeable consequences to others of that tasking. Before authorising the use or conduct of a CHIS, the authorising officer should ensure that a risk assessment is carried out to determine the risk to the CHIS of any tasking and the likely consequences should the role of the CHIS become known. The ongoing security and welfare of the CHIS, after the cancellation of the authorisation, should also be considered at the outset. Also, consideration should be given to the management of any requirement to disclose information tending to reveal the existence or identity of a CHIS to, or in, Court.

6.15 The CHIS handler is responsible for bringing to the attention of the CHIS controller any concerns about the personal circumstances of the CHIS, insofar as they might affect:

- the validity of the risk assessment;
- the conduct of the CHIS; and
- the safety and welfare of the CHIS.

6.16 Where appropriate, concerns about such matters must be considered by the authorising officer, and a decision taken on whether or not to allow the authorisation to continue.

Chapter 7

KEEPING OF RECORDS

Centrally retrievable record of authorisations

7.1 A centrally retrievable record of all authorisations should be held by each public authority. These records need only contain the name, code name, or unique identifying reference of the CHIS, the date the authorisation was granted, renewed or cancelled and an indication as to whether the activities were self-authorised. These records should be updated whenever an authorisation is granted, renewed or cancelled and should be made available to the relevant Commissioner or an Inspector from the Office of Surveillance Commissioners upon request. These records should be used when calculating the period of deployment for the purposes of the 2013 Order. These records should be retained for a period of at least five years from the ending of the authorisations to which they relate.

7.2 While retaining such records for the time stipulated, public authorities must take into consideration the duty of care to the CHIS, the likelihood of future criminal or civil proceedings relating to information supplied by the CHIS or activities undertaken, and specific rules relating to data retention, review and deletion under the Data Protection Act and, where applicable, the Code of Practice on the Management of Police Information.

7.3 Records must be retained to allow the Investigatory Powers Tribunal, established under Part IV of the Act, to carry out its functions. The Tribunal will consider complaints made up to one year after the conduct to which the complaint relates and, where it is equitable to do so, may consider complaints made more than one year after the conduct to which the complaint relates (see section 67(5) of the Act), particularly where continuing conduct is alleged. It is thus desirable if possible to retain records for up to five years.

Individual records of authorisation and use of CHIS

7.4 Detailed records must be kept of the authorisation and use made of a CHIS. Section 29(5) of the 2000 Act provides that an authorising officer must not grant an authorisation for the use or conduct of a CHIS unless they believe that there are arrangements in place for ensuring that there is at all times a person with the responsibility for maintaining a record of the use made of the CHIS. The Regulation of Investigatory Powers (Source Records) Regulations 2000; SI No. 2725 details the particulars that must be included in these records.

7.5 Public authorities are encouraged to consider maintaining such records also for human sources who do not meet the definition of a CHIS. This may assist authorities to monitor the status of a human source and identify whether that source becomes a CHIS.

Further documentation

7.6 In addition, records or copies of the following, as appropriate, should be kept by the relevant authority for at least five years:

- a copy of the authorisation together with any supplementary documentation and notification of the approval given by the authorising officer;
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- the reason why the person renewing an authorisation considered it necessary to do so;
- any authorisation which was granted or renewed orally (in an urgent case) and the reason why the case was considered urgent;
- any risk assessment made in relation to the CHIS;
- the circumstances in which tasks were given to the CHIS;
- the value of the CHIS to the investigating authority;
- a record of the results of any reviews of the authorisation;
- the reasons, if any, for not renewing an authorisation;
- the reasons for cancelling an authorisation;
- the date and time when any instruction was given by the authorising officer that the conduct or use of a CHIS must cease; and

- a copy of the decision by an Ordinary Commissioner on the renewal of an authorisation beyond 12 months.

7.7 The records kept by public authorities should be maintained in such a way as to preserve the confidentiality, or prevent disclosure of the identity of the CHIS, and the information provided by that CHIS.

Chapter 8

HANDLING OF MATERIAL

Retention and destruction of material

8.1 Each public authority must ensure that arrangements are in place for the secure handling, storage and destruction of material obtained through the use or conduct of a CHIS. Authorising officers must ensure compliance with the appropriate data protection requirements under the Data Protection Act 1998 and any relevant codes of practice produced by individual authorities relating to the handling and storage of material.

8.2 Where the product of the use or conduct of a CHIS could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with applicable disclosure requirements.

8.3 Subject to the provisions in Chapter 4 above, there is nothing in the 2000 Act or this code of practice which prevents material obtained from authorisations for the use or conduct of a CHIS for a particular purpose from being used to further other purposes.

Law enforcement agencies

8.4 In the case of the law enforcement agencies, particular attention is drawn to the requirements of the code of practice issued under the Criminal Procedure and Investigations Act 1996. This requires that material which is obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained.

The intelligence services, MOD and HM forces

8.5 The heads of these agencies are responsible for ensuring that arrangements exist to make sure that no information is stored by the authorities, except as necessary for the proper discharge of their functions. They are also responsible for arrangements to control onward disclosure. For the intelligence services, this is a statutory duty under the 1989 Act and the 1994 Act.

8.6 With regard to the service police forces (the Royal Navy Police, the Royal Military Police and the Royal Air Force Police), particular attention is drawn to the Criminal Procedure and Investigations Act 1996 (Code of Practice) (Armed Forces) Order 2008, which requires that the investigator retain all material obtained in a service investigation which may be relevant to the investigation.

Use of material as evidence

8.7 Subject to the provisions in Chapter 4 above, material obtained from a CHIS may be used as evidence in criminal proceedings.¹⁶ The admissibility of evidence is governed by the common law, the Civil Procedure Rules, section 78 of the Police and Criminal Evidence Act 1984¹⁷ and the Human Rights Act 1998. Whilst this code does not affect the application of those rules, obtaining appropriate authorisations should help ensure the admissibility of evidence derived from CHIS.

8.8 Product obtained by a CHIS is subject to the ordinary rules for retention and disclosure of material under the Criminal Procedure and Investigations Act 1996, where those rules apply to the law enforcement body in question.

8.9 There are also well-established legal procedures under public interest immunity provisions that can be applied when seeking to protect the identity of a source from disclosure in such circumstances.

¹⁶ Whether these proceedings are brought by the public authority that obtained the authorisation or by another public authority (subject to handling arrangements agreed between the authorities).

¹⁷ And section 76 of the Police & Criminal Evidence (Northern Ireland) Order 1989.

Chapter 9

SENIOR RESPONSIBLE OFFICERS AND OVERSIGHT BY COMMISSIONERS

The senior responsible officer

9.1 Within every relevant public authority a senior responsible officer must be responsible for:

- the integrity of the process in place within the public authority for the management of CHIS;
- compliance with Part II of the Act and with this code;
- oversight of the reporting of errors to the relevant oversight Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- engagement with the OSC inspectors when they conduct their inspections, where applicable; and
- where necessary, oversight of the implementation of post-inspection action plans approved by the relevant oversight Commissioner.

9.2 Within local authorities, the senior responsible officer should be a member of the corporate leadership team and should be responsible for ensuring that all authorising officers are of an appropriate standard in light of any recommendations in the inspection reports prepared by the Office of the Surveillance Commissioner. Where an inspection report highlights concerns about the standards of authorising officers, this individual will be responsible for ensuring the concerns are addressed.

Oversight by Commissioners

9.3 The 2000 Act requires the Chief Surveillance Commissioner to keep under review (with the assistance of the Surveillance Commissioners and Assistant Surveillance Commissioners) the

performance of functions under Part III of the 1997 Act and Part II of the 2000 Act by the police (including the service police forces, the Ministry of Defence Police and the British Transport Police), NCA, HMRC and the other public authorities listed in Schedule 1 of the 2000 Act and the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010, and in Northern Ireland officials of the Ministry of Defence and HM Forces.

9.4 The Intelligence Services Commissioner's remit is to provide independent oversight of the use of Part II of the 2000 Act and the 1994 Act by the Security Service, Secret Intelligence Service, GCHQ and the Ministry of Defence and HM Forces (excluding the service police forces, and in Northern Ireland officials of the Ministry of Defence and HM Forces).

9.5 This code does not cover the exercise of any of the Commissioners' functions. It is the duty of any person who uses Part II of RIPA to comply with any request made by a Commissioner to disclose or provide any information requested for the purpose of enabling the Commissioner to carry out their functions.

9.6 References in this code to the performance of review functions by the Chief Surveillance Commissioner and other Commissioners apply also to Inspectors and other members of staff to whom such functions have been delegated.

9.7 Reports made by the Commissioners concerning the inspection of public authorities and their exercise and performance of powers under Part II may be made available by the Commissioners to the Home Office to promulgate good practice and help identify training requirements within public authorities.

9.8 Subject to the approval of the relevant Commissioner public authorities may publish their inspection reports, in full or in summary, to demonstrate both the oversight to which they are subject and their compliance with Part II of the Act and this code. Approval should be sought on a case by case basis at least 10 working days prior to intended publication, stating whether the report is to be published in full, and if not stating which parts are to be published or how it is to be summarised.

Chapter 10

COMPLAINTS

10.1 The 2000 Act establishes an independent Tribunal. This Tribunal will be made up of senior members of the judiciary and the legal profession and is independent of the Government. The Tribunal has full powers to investigate and decide any case within its jurisdiction. This code does not cover the exercise of the Tribunal's functions. Details of the relevant complaints procedure can be obtained from the following address:

Investigatory Powers Tribunal

PO Box 33220

London

SW1H 9ZQ

 020 7035 3711

Annex A

Authorisation levels when knowledge of confidential information is likely to be acquired or when a vulnerable individual or juvenile is to be used as a source

Relevant public authority	Authorisation level when knowledge of confidential information is likely to be acquired	Authorisation level for when a vulnerable individual or a juvenile is to be used as a source
Police Forces:		
Any police force maintained under section 2 of the Police Act 1996 (police forces in England and Wales outside London)	Chief Constable	Asst Chief Constable
The Police Service of Scotland	Chief Constable	Asst Chief Constable
The Metropolitan police force	Asst Commissioner	Commander
The City of London police force	Commissioner	Commander
The Police Service of Northern Ireland	Dept Chief Constable	Asst Chief Constable
The Ministry of Defence Police	Chief Constable	Asst Chief Constable

Relevant public authority	Authorisation level when knowledge of confidential information is likely to be acquired	Authorisation level for when a vulnerable individual or a juvenile is to be used as a source
The Royal Navy Police	Provost Marshal	Provost Marshal
The Royal Military Police	Provost Marshal	Provost Marshal
The Royal Air Force Police	Provost Marshal	Provost Marshal
The National Crime Agency	Deputy Director General	Deputy Director
The Serious Fraud Office	A Member of the Senior Civil Service or Head of Domain	A Member of the Senior Civil Service or Head of Domain
The Intelligence Services:		
The Security Service	Deputy Director General	Deputy Director General
The Secret Intelligence Service	A Director of the Secret Intelligence Service	A member of the Secret Intelligence Service not below the equivalent rank to that of a Grade 5 in the Home Civil Service
The Government Communications Headquarters	A Director of GCHQ	A Director of GCHQ

Relevant public authority	Authorisation level when knowledge of confidential information is likely to be acquired	Authorisation level for when a vulnerable individual or a juvenile is to be used as a source
HM Forces:		
The Royal Navy	Rear Admiral	Rear Admiral
The Army	Major General	Major General
The Royal Air Force	Air-Vice Marshal	Air-Vice Marshal
The Commissioners for HM Revenue and Customs	Director Investigation, or Regional Heads of Investigation	Grade 7 (Intel)
The Department for the Environment, Food and Rural Affairs:		
DEFRA Investigation Services	Head of DEFRA Investigation Service	Head of DEFRA Investigation Service
Marine and Fisheries Agency	Head of Better Regulation	—
Centre for Environment, Fisheries & Aquaculture Science	Head of Better Regulation	Head of Better Regulation
The Department of Health:		
The Medicines & Healthcare Products Regulatory Agency	Chief Executive	Head of Division for Inspection and Enforcement

Relevant public authority	Authorisation level when knowledge of confidential information is likely to be acquired	Authorisation level for when a vulnerable individual or a juvenile is to be used as a source
The Home Office	Senior Civil Servant pay band 1 with responsibility for criminal investigations in relation to immigration and border security	Grade 6 with responsibility for criminal investigations in relation to immigration and border security
The Ministry of Justice	Chief Executive Officer of the National Offender Management Service	A member of the Senior Civil Service in the National Offender Management Service not below the equivalent rank of a Grade 5 in the Home Civil Service
The Northern Ireland Office:		
The Northern Ireland Prison Service	Director or Deputy Director Operations in the Northern Ireland Prison Service	Director or Deputy Director Operations in the Northern Ireland Prison Service

Relevant public authority	Authorisation level when knowledge of confidential information is likely to be acquired	Authorisation level for when a vulnerable individual or a juvenile is to be used as a source
The Department of Business, Innovation and Skills	The Director of Legal Services A	The Director of Legal Services A
The Welsh Assembly Government	Head of Department for Health & Social Services, Head of Department for Health & Social Services Finance, Head of Rural Payments Division, Regional Director or equivalent grade in the Care & Social Services Inspectorate for Wales	Head of Department for Health & Social Services, Head of Department for Health & Social Services Finance, Head of Rural Payments Division, Regional Director or equivalent grade in the Care & Social Services Inspectorate for Wales

Relevant public authority	Authorisation level when knowledge of confidential information is likely to be acquired	Authorisation level for when a vulnerable individual or a juvenile is to be used as a source
Any county council or district council in England, a London borough council, the Common Council of the City of London in its capacity as a local authority, the Council of the Isles of Scilly, and any county council or borough council in Wales	Head of Paid Service, or (in his absence) the person acting as the Head of Paid Service	Head of Paid Service, or (in his absence) the person acting as the Head of paid Service
The Environment Agency	Chief Executive of the Environment Agency	Executive Manager in the Environment Agency
The Prudential Regulation Authority	Chief Executive of the Prudential Regulation Authority	Chief Executive of the Prudential Regulation Authority
The Competition and Markets Authority	Chair of the Competition and Markets Authority	Chair of the Competition and Markets Authority
The Financial Conduct Authority	Chairman of the Financial Conduct Authority	Chairman of the Financial Conduct Authority

Relevant public authority	Authorisation level when knowledge of confidential information is likely to be acquired	Authorisation level for when a vulnerable individual or a juvenile is to be used as a source
The Food Standards Agency	Head of Group, or Deputy Chief Executive or Chief Executive of the Food Standards Agency	Head of Group, or Deputy Chief Executive or Chief Executive of the Food Standards Agency
The Gambling Commission	—	Chief Executive
The Health and Safety Executive	Director of Field Operations, or Director of Hazardous Installations Directorate	Director of Field Operations, or Director of Hazardous Installations Directorate

Annex B

Authorisation levels for the enhanced arrangements set out in the Regulation of Investigatory Powers (Covert Human Intelligence Sources: Relevant Sources) Order 2013

(1) Relevant public authorities	(2) Prescribed offices etc.	(3) Urgent cases	(4) Grounds set out in section 29(3) of the Act
A police force maintained under section 2 of the Police Act 1996	Relevant Source Authorisation Assistant Chief Constable Long-Term Authorisation Chief Constable	Superintendent	Paragraphs (a), (b), (c), (d) and (e)
The City of London Police Force	Relevant Source Authorisation Commander Long-Term Authorisation Commissioner	Superintendent	Paragraphs (a), (b), (c), (d) and (e)

(1) Relevant public authorities	(2) Prescribed offices etc.	(3) Urgent cases	(4) Grounds set out in section 29(3) of the Act
The Metropolitan Police Force	Relevant Source Authorisation Commander Long-Term Authorisation Assistant Commissioner	Superintendent	Paragraphs (a), (b), (c), (d) and (e)
The Police Service of Northern Ireland	Relevant Source Authorisation Assistant Chief Constable Long-Term Authorisation Chief Constable	Superintendent	Paragraphs (a), (b), (c), (d) and (e)
The Police Service of Scotland	Relevant Source Authorisation Assistant Chief Constable Long-Term Authorisation Chief Constable	Superintendent	Paragraphs (a), (b), (c), (d) and (e)

(1) Relevant public authorities	(2) Prescribed offices etc.	(3) Urgent cases	(4) Grounds set out in section 29(3) of the Act
The Ministry of Defence Police	Relevant Source Authorisation Assistant Chief Constable Long-Term Authorisation Chief Constable	Superintendent	Paragraphs (a), (b) and (c)
The Royal Navy Police	Relevant Source Authorisation Commander Long-Term Authorisation Provost Marshal (Navy)	Lieutenant Commander	Paragraphs (a), (b) and (c)
The Royal Military Police	Relevant Source Authorisation Colonel Long-Term Authorisation Provost Marshal (Army)	Major	Paragraphs (a), (b) and (c)

(1) Relevant public authorities	(2) Prescribed offices etc.	(3) Urgent cases	(4) Grounds set out in section 29(3) of the Act
The Royal Air Force Police	Relevant Source Authorisation Wing Commander Long-Term Authorisation Provost Marshal (Royal Air Force)	Squadron Leader	Paragraphs (a), (b) and (c)
The British Transport Police	Relevant Source Authorisation Assistant Chief Constable Long-Term Authorisation Chief Constable	Superintendent	Paragraphs (a), (b), (c), (d) and (e)
The National Crime Agency	Relevant Source Authorisation Deputy Director Long-Term Authorisation Deputy Director General	Grade 2 Senior Manager	Paragraph (b)

(1) Relevant public authorities	(2) Prescribed offices etc.	(3) Urgent cases	(4) Grounds set out in section 29(3) of the Act
Her Majesty's Revenue and Customs	Relevant Source Authorisation Assistant Director Long-Term Authorisation Director Criminal Investigation	Senior Officer	Paragraphs (a), (b), (d), (e) and (f)

(1) Relevant public authorities	(2) Prescribed offices etc.	(3) Urgent cases	(4) Grounds set out in section 29(3) of the Act
The Home Office	<p>Relevant Source Authorisation Senior Civil Service pay band 1 with responsibility for criminal investigations in relation to immigration and border security</p> <p>Long-Term Authorisation Director General with responsibility for criminal investigations in relation to immigration and border security</p>	Grade 6 with responsibility for criminal investigations in relation to immigration and border security	Paragraphs (b), (c) and (d)

This code of practice provides guidance and rules on authorisations for the use or the conduct of covert human intelligence sources under Part 2 of the Regulation of Investigatory Powers Act 2000. It sets out the authorisation procedures to be followed for the grant, review, renewal and cancellation of authorisations, and for the management of sources, as well as special rules for authorisations in respect of confidential and legally privileged information or juvenile sources.

The code is aimed primarily at members of public authorities involved in making applications for the grant of authorisations and those persons designated to grant authorisations.

Appendix 4

Unique Reference Number	To be allocated by Democratic Governance
--------------------------------	--

RIP 1 - APPLICATION (AIDE MEMOIRE)

REGULATION OF INVESTIGATORY POWERS ACT 2000 PART II APPLICATION FOR AUTHORITY FOR DIRECTED SURVEILLANCE

The CFO will complete the form prior to starting surveillance. The three month authorisation period starts from the date shown in box 11 and will be reviewed, as a minimum, on a monthly basis.

Public Authority (Including full address)	Blackpool Council Enter full postal address
---	--

Name of applicant	Details of the person completing the form	Directorate	
Full Address	Provide the full postal address of your Directorate		
Contact Details	Provide full contact details, including email address. Make it easy for the Authorising Officer, or anyone else associated with the process to contact you.		
Investigation/ Operation Name	This may be an investigation reference number allocated to this case, or some other reference.		
Investigating Officer (if a person other than the applicant)	If someone who is not the investigator is completing the form, then the investigators details must be put in this box.		

Unique Reference Number	To be allocated by Democratic Governance
--------------------------------	--

Details of the Application
1. Give grade or position of Authorising Officer in accordance with Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 No. 521
The exact position of the Authorising Officer should be given e.g. Chief Internal Auditor.
2. Describe the purpose of the specific operation of investigation.
<p>Describe the investigation to date including the offences and the relevant legislation. When, where and how are the offences occurring. Remember the Authorising Officer needs to be clear what the offence is and the circumstances (keep information relevant and to the point).</p> <p>Include the details of the suspects and persons involved and the role they play within the investigation. (Do not put confidential information in such as informants' names).</p> <p>Consider disclosure implications under CPIA about not revealing unnecessary information. However, the Authorising Officer needs sufficient relevant information to make a decision. The provisions of using CPIA sensitive information may be a way of dealing with the sensitivity issues later, by editing material if it has to be disclosed. However, if the document contains sensitive information remember to keep it secure at all times.</p> <p>Cross-reference where necessary to other relevant applications.</p> <p>Refer to the evaluation of the intelligence, as the Authorising Office should consider it provenance and value.</p> <p>WHEN MENTIONING THE OFFENCE REMEMBER IT MUST BE AS PER BOX 6</p>

Unique Reference Number	To be allocated by Democratic Governance
--------------------------------	--

3. Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, recorder) that may be used.

This should be completed, after attending the area of where the activity is to be carried out. A surveillance assessment should be completed, taking into account risks or limiting factors. (Limiting factors are anything that can affect the success of the operation).

Consider the Authorising Officer statement in Box 12, the five Who, What, Where, When, Why and How? The applicant can only do what is authorised by the Authorising Officer, not what they have applied for.

Consider the aims and objective, confirmation of address may only need static observations, however lifestyle intelligence may require foot/mobile and use of covert cameras etc.

What exactly do you want to do? Is it static observations, foot or mobile? Do you want a combination? However, only ask for what you can realistically carry out. It is not a wish list, it should be carried out to achieve the objectives.

How do you want to carry out the surveillance and what equipment do you want to use? You must make the Authorising Officer aware of the capabilities of any equipment you want to use.

Where is the activity to take place? Who is the activity against and when do you want to carry it out?

What is the expected duration? It does not mean that it must only be authorised to this point. Once signed, the authorisation last for a three-month period. You must update the Authorising Officer when they set the review dates. If your operation ends prior to any review date or the three-month period, you must cancel it straight away and submit the cancellation form (RIP 3). It does not expire.

THIS IS NOT A WISH LIST, IT SHOULD BE THOUGHT THROUGH

REMEMBER YOU CAN ONLY DO WHAT IS AUTHORISED ON THE AUTHORISING SECTION, NOT WHAT YOU HAVE APPLIED FOR IN THIS SECTION.

Unique Reference Number	To be allocated by Democratic Governance
--------------------------------	--

4. The identities, where known, of those to be subject of the directed surveillance.

- **Name**
- **Address:**
- **DOB:**
- **Other information as appropriate**

If you do not know who the subjects are, insert any description you may have. If as a result of the surveillance, you identify anyone, you must submit this information on a review form to the Authorising Officer.

Consider any known associates. If the intelligence is that the subject of the surveillance has known associates, are they likely to become subjects of the surveillance? If so, detail them as part of the application.

5. Explain the information that is desired to obtain as a result of the directed surveillance.

These are the surveillance objectives. They should have been identified during the planning stage and a feasibility study carried out to assess whether they can be achieved. It is no use setting objective that cannot be achieved.

- What is the surveillance going to tell you?
- What, if any, criminality will it establish?
- Will it identify subjects involved in criminality?
- Will it house subject or their criminal associates?

Example:

- Identify the location of the subject's place of work
- To gather information and evidence to establish the extent of the criminality
- Identify other persons involved, such as suppliers
- Identify other premises involved, such as storage buildings
- Obtain best evidence with photographic equipment to assist with identifying the offenders.

Obtain best evidence to assist with a prosecution of offenders.

Unique Reference Number	To be allocated by Democratic Governance
--------------------------------	--

6. Identify on which grounds the directed surveillance is necessary under Section 28(3) of RIPA.

Delete those that are not applicable. Ensure that you know which grounds you are entitled to rely on (SI 2010 No.521)

- In the interests of national security;
- For the purpose of preventing or detecting crime or of preventing disorder;
- In the interests of the economic well-being of the United Kingdom;
- In the interests of public safety;
- For the purpose of protecting public health
- For the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department.

For Directed Surveillance, Local Authorities only lawful purpose is preventing or detecting crime and the crime must be capable of carrying six month imprisonment or criminal offences relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A of the Licencing Act 2003 or section 7 if the Children and Young Persons Act 1933.

Due to the nature of the offence, if any other area above is applicable such as protection of public health, this should be made clear in the body of the application and the proportionality section.

7. Explain why this directed surveillance is necessary on the grounds you have identified.

Code paragraph 3.3.

You can reiterate the offence and its penalty to show lawfulness.

Do not say this is the only way to achieve the objective. You have to justify why it is by explaining what other enquiries have been carried out and the results? This does not have to be a last resort, but if there is a less intrusive way of achieving your objective you should take that option, or explain why you cannot take that option.

Why is it necessary at this stage of the enquiry to carry out covert activity?

What is the purpose of the operation?

How will the activity assist or progress the investigation?

What will be the consequences of the proposed action be to the victim?

Why do we need this evidence/ intelligence/ information?

Consequences of not taking action

It is not for the applicant to state on the application that they believe it to be necessary.

This is the responsibility of the Authorising Officer to reach that decision.

8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. Describe precautions you will take to minimise collateral intrusion.

Code paragraphs 3.8 to 3.11.

There are three parts to this section. You must answer them all, as this section directly impacts upon the proportionality test.

1. Supply Details of Potential Collateral Intrusion

Visit the location of where the activity is to take place and carry out a risk assessment. Who lives at the property that you may be watching. Have they got children who might be affected such as going to school?

Determine where you need to be carrying out the surveillance. What else can you see? What equipment will you be using and what will it see and record?

Consider confidential information. It may be useful to paint the picture in words of what it is you will be watching in the locality. This will assist the Authorising Officer. You may also want to refer to any plans or maps attached to the application.

2. Why is the intrusion unavoidable?

Consider why the intrusion is unavoidable, such as the location and time frame that the observations have to be carried out. It may be that you are limited to the use of certain equipment only and therefore governed by its operating capabilities. Your observation position may be the only place you can use.

3. Describe the precautions you will take to minimise collateral intrusion

Having carried out the risk assessment and identified what the intrusion is, consider ways of reducing the intrusion, or keeping it to a minimum. You should consider:

State who the activity will be focused on, such as the subject etc., not the innocent third parties subject to the collateral intrusion.

Keeping the surveillance activity focussed with regards to length of time spent on the observations. However, remember that you still need to achieve your objectives. You will need some flexibility built into your timings.

If using technical equipment such as video or covert recordings, consider the position and focal length of the lenses when filming to reduce the intrusion. Consider when and who you will use the equipment against, such as the suspects only.

Unique Reference Number	To be allocated by Democratic Governance
--------------------------------	--

How will you manage any images obtained? Consider Data Protection, confidentiality, security, dissemination of the images and any guidance provided by your organisation, including any Home Office guidance.

Are the staff trained to carry out the activity? If so, this may assist, as they should know what they doing with regards to collateral intrusion.

The activity needs to be tightly managed and reviewed constantly. If there is a considerable change in the intrusion once the activity commences, then the Authorising Officer needs to be made aware.

9. Explain why the directed surveillance is proportionate to what it seeks to achieve.

How intrusive might it be on the subject of surveillance or on others?
 Why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means?
 Code paragraphs 3.4 to 3.7

How serious are the offences under investigation? What is the direct or accumulative consequence of the offences?

What are the effect of the offences on the victim or the consequences of what is happening?

Are you asking to do a lot to achieve a little? Do not use a sledgehammer to crack a nut!

If you have provided a good explanation of how the intrusion will be reduced and managed in the collateral intrusion box, refer them to it.

Explain why you need to undertake this activity to achieve your objectives, against using other methods. Why, in operational terms, does your need to use the activity (how the activity will progress the investigation) out weigh the level of intrusion? Why is this method the least intrusive option?

Are your methods/ tactics balanced in relation to the likely results?

Consider the length of time the surveillance operation.

What methods are required to achieve the objectives and are the any less intrusive

Unique Reference Number	To be allocated by Democratic Governance
--------------------------------	--

methods? You should explain what if any less intrusive methods have been considered. If they can be used they should be. If however less intrusive methods cannot be used, explain why. You should also account that technical surveillance may be more intrusive.

Consequences of not taking action.

10. Confidential Information (indicate the likelihood of acquiring any confidential material)

Is there any likelihood of Health, Solicitors, Counselling and Spiritual etc.?

It is unlikely that you will obtain this type of material, but an assessment should take place. If you are, it is a higher level of Authorising Officer who needs to consider it.

Do not mix this up with Private Information which is part of the consideration when assessing whether the activity falls under RIPA

Confidential material consists of:

- Matters subject to Legal Privilege
- Confidential Person Information
- Confidential Journalistic material

Section 3 of the current Home Office Code of Practice gives a detailed explanation for each of the above.

Put No or None. Do not mention not likely.

11. Applicants Details

Name (print)		Telephone number:	
Grade/Rank:		Date:	
Signature:			

Unique Reference Number	To be allocated by Democratic Governance
--------------------------------	--

12. Authorising Officer's Statement.

I hereby authorise directed surveillance defined as follows:

Spell out the five w's – who, what, where, why and how.

Remember that each case has to be assessed on its own merits

Who are you authorising to carry out the activity? Are the staff from one office? Or if a joint operation, please state that fact and name the organisation. You have to actually authorise the other organisation's staff in writing.

What are you authorising them to do and what equipment are you authorising them to use? You should have knowledge of the equipment's capability

Who are you authorising them to do it against, person, address, vehicle etc.?

When are you authorising them to do it?

Where are you authorising the activity to take place?

Why are you authorising whatever you are allowing them to do? They should have stated within the application earlier what they are hoping to achieve.

When authorising the activity it is live for three months, you cannot authorise for less.

You should set a review date for you to review it if you think that the surveillance should be a shorter period.

If the case has been discussed with the applicant, record the details

If not authorising, state why.

13. Explain why you (as Authorising Officer) believe directed surveillance is necessary

There are five areas to be considered:

Code 3.3 – requires that the person granting an authorisation BELIEVES that the authorisation is necessary in the circumstances of the particular case for one of the statutory reasons (see box 6). Have they made clear what the offence or offences are in the body of the application?

Code 3.4 – then if the activities are necessary, the person granting the authorisation must BELIEVE that they are proportionate to what is sought to be achieved by carrying them out. You must BELIEVE that the objective cannot be met by other less intrusive means.

Unique Reference Number	To be allocated by Democratic Governance
--------------------------------	--

Sec 72 RIPA 2000 – a person exercising or performing any power or duty in relation to which provision may be made by a code of practice under section 71 shall, in doing so, HAVE REGARD TO THE PROVISIONS (so far they are applicable) of every code of practice for the time being in force under that section.

Collateral Intrusion Code of Practice 3.8 – before authorising surveillance the authorising officer should also TAKE INTO ACCOUNT the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation.

Code of Practice 3.15 – any person granting or applying for an authorisation will also NEED TO BE AWARE of particular sensitivities in the local community where the surveillance is taking place and of similar activities being undertaken by other public authorities, which could impact on the deployment of surveillance.

This will take some consideration. Read and study the application fully. Refer to the applicants boxes that deal with these issues.

Detail your thought process, how have you come to the conclusion. If you are making decisions from reading supporting material, mention the supporting material and keep a copy in the central register.

Make your decision on written material and not discussions with the case office, which may be difficult to justify at a later date at Court.

14. Confidential material authorisation

Supply detail demonstrating compliance with Code paragraphs 4.1 to 4.31

This is completed by the Authorising Officer who has responsibility to consider the authorisation if confidential information is likely to be obtained. (Usually, this will be someone of a much higher position, e.g. Chief Executive).

Unique Reference Number	To be allocated by Democratic Governance
--------------------------------	--

15. Date of First Review	<p>The Authorising Officer must set the review date. However, it must be from the date approved by the Magistrate.</p> <p>Consider what the applicant has stated regarding the length of time required. Remember, this is so you as the Authorising Officer can now review the need for the activity to continue on the date you have set. Also refer to policy, most state that it must not be longer than a month. However, you must assess it against all the facts.</p>		
Programme for subsequent review of this authorisation.			
Code Paragraph 3.23.			
Only complete this box if review dates after the first review are known. If not, or inappropriate to set additional review dates then leave blank.			
Name (print)		Grade/ Rank	
Signature		Date and Time	
Expiry date and Time:		This will be three months after the Magistrate has approved it.	

The layout and guidance of this RIP form is subject to change upon receipt of the definitive Home Office Code of Practice. Any changes to procedures, guidance or to the series of RIP forms will be notified in writing – **do we need this? What does it mean?**

Unique Reference Number	To be allocated by Democratic Governance
--------------------------------	--

RIP 2 – RENEWALS

PART II OF THE REGULATION OF INVESTIGATORY POWERS ACT 2000

RENEWAL OF A DIRECTED SURVEILLANCE AUTHORISATION

Public Authority (Including full address)	Blackpool Council Enter full postal address
---	--

Name of applicant	Details of the person completing the form	Directorate	
Full Address	Provide the full postal address of your Directorate		
Contact Details	Provide full contact details, including email address. Make it easy for the Authorising Officer, or anyone else associated with the process to contact you.		
Investigation/ Operation Name	This may be an investigation reference number allocated to this case, or some other reference.		
Renewal Number	ENTRY: Show 1, 2 OR 3 depending on whether the renewal application is the first or subsequent.		

**Unique Reference
Number**

To be allocated
by Democratic
Governance

1. Renewal numbers and dates of any previous renewals.	
Renewal Number	Date
Enter the number of each PREVIOUS renewal	Enter the date that refers to the date of the PREVIOUS Renewal signed by the Authorising Officer
2. Detail any significant changes to the information as listed in the original authorisation as it applies at the time of the renewal.	
<p>Review boxes 2 to 7 of the RIP 1 (Authorisation) and record ANY changes for the individual case this will enable the Authorising Officer to determine whether continuing the surveillance is still necessary and appropriate in light of any details noted.</p> <p>With the introduction of RIP 5 (Change of Circumstances), the likelihood of needing to complete this box is rare, other than to refer the Authorising Officer to the previously completed RIP 5(s).</p> <p>However, there may be some circumstances in which completion is appropriate (e.g. a change that occurs at around 10 days before the need to cancel a RIPA).</p>	
3. Detail the reasons why it is necessary to continue with the directed surveillance.	
<p>Details must be specific as to why it is still necessary to continue surveillance and include what is to be achieved by further surveillance. Will it add value? What would a decision maker think?</p>	
4. Detail why the directed surveillance is still proportionate to what it seeks to achieve.	
Empty space for content	

Unique Reference Number

To be allocated by Democratic Governance

5. Indicate the content and value to the investigation or operation of the information so far obtained by the directed surveillance.

Explain what has been achieved so far and how useful it is to the investigation. This will indicate to the Authorising Officer whether further surveillance is necessary.

6. Give details of the results of the regular reviews of the investigation or operation.

7. Applicant's Details

Name (Print)		Tel No	
Grade/Rank		Date	
Signature			

8. Authorising Officer's Comments. This box must be completed.

Comments should include what consideration has been given to the application and why further authorisation of surveillance is or is not appropriate.

The Authorising Officer should record when the first review of the case should take place, taking into account the information in box 5.

Reviews must take place at intervals not longer than one month, but depending on the circumstances of the case, reviews can be conducted more frequently.

**Unique Reference
Number**

To be allocated
by Democratic
Governance

9. Authorising Officer's Statement.

I, [insert name], hereby authorise the renewal of the directed surveillance operation as detailed above. The renewal of this authorisation will last for 3 months unless renewed in writing.

This authorisation will be reviewed frequently to assess the need for the authorisation to continue.

Name (Print)			Grade / Rank	
Signature			Date	
Renewal From:	Time:		Date:	
Date of first review.				
Date of subsequent reviews of this authorisation.				

Unique Reference Number	To be allocated by Democratic Governance
--------------------------------	--

RIP 3 – CANCELLATION (AIDE MEMOIRE)

REGULATION OF INVESTIGATORY POWERS ACT 2000 PART II CANCELLATION OF A DIRECTED SURVEILLANCE

Public Authority (Including full address)	Blackpool Council Enter full postal address
---	--

Name of applicant	Details of the person completing the form	Directorate	
Investigation/ Operation Name	This may be an investigation reference number allocated to this case, or some other reference.		

Details of the Cancellation	
1. Explain the reason(s) for the cancellation of the authorisation	
<p>Give a full explanation as to why it is no longer necessary to continue surveillance. Examples are:</p> <ul style="list-style-type: none"> • objective(s) established? if not, why? • objective(s) achieved by means other than surveillance? • subject(s) no longer part of investigation? <p>(this list is not exhaustive)</p>	
2. Explain the value of surveillance in the operation	
<p>What was achieved as a result of the authorisation for surveillance, with reference to box 5 of the RIP 1 (Authorisation) or box 3 of the RIP 2 (Review)?</p> <p>If there was no value to the surveillance, explain why.</p>	

Unique Reference Number	To be allocated by Democratic Governance
--------------------------------	--

Compare what you have now with what you wanted on RIP 1.

What has been achieved?

What has not been achieved and why?

3. Authorising officer's statement.

I, [insert name], hereby authorise the cancellation of the directed surveillance investigation/operation as detailed above.

Name (Print)		Grade	
Signature		Date	

4. Time and Date of when the authorising officer instructed the surveillance to cease.

Date:		Time:	
--------------	--	--------------	--

5. Authorisation cancelled.

Date:		Time:	
--------------	--	--------------	--

Unique Reference Number	To be allocated by Democratic Governance
--------------------------------	--

RIP 4 – REVIEW (AIDE MEMOIRE)

**PART II OF THE REGULATION OF INVESTIGATORY POWERS ACT 2000
REVIEW OF A DIRECTED SURVEILLANCE AUTHORISATION**

Public Authority (Including full address)	Blackpool Council Enter full postal address
---	--

Name of applicant	Details of the person completing the form	Directorate	
Full Address	Provide the full postal address of your Directorate		
Contact Details	Provide full contact details, including email address. Make it easy for the Authorising Officer, or anyone else associated with the process to contact you.		
Operation Name			
Date of authorisation or last renewal		Expiry date of authorisation or last renewal	
Review Number			

Details of the Review

1. Review number and dates of any previous reviews.	
Review Number	Date

2. Summary of the investigation/operation to date, including what information has been obtained and the value of the information so far obtained.

Unique Reference Number	To be allocated by Democratic Governance
--------------------------------	--

3. Detail the reasons why it is necessary to continue using Direct Surveillance.
4. Explain how the proposed activity is still proportionate to what it seeks to achieve.
5. Detail any incidents of collateral intrusion and the likelihood of any further incidents of collateral intrusions occurring.
6. Give details of any confidential information acquired or accessed and the likelihood of acquiring confidential information.

7. Applicants Details			
Name (print)		Telephone number:	
Grade/Position:		Date:	
Signature:			

8. Review Officer's Comments, including whether or not the use or conduct of the source should continue?

Unique Reference Number	To be allocated by Democratic Governance
--------------------------------	--

9. Authorising Officer's Statement			
I, _____, hereby agree that the directed surveillance investigation/operation as detailed above [should/should not] continue [until its next review/renewal][it should be cancelled immediately].			
Name (print)		Grade/Position:	
Signature		Date:	

10. Date of next Review	
--------------------------------	--

Unique Reference Number	To be allocated by Democratic Governance
--------------------------------	--

RIP 5 – NON RIPA APPLICATION (AIDE MEMOIRE)

REGULATION OF INVESTIGATORY POWERS ACT 2000 PART II APPLICATION FOR AUTHORITY FOR SURVEILLANCE

The Line Manager will complete the form prior to starting surveillance. The surveillance period starts from the date shown in Box 8 and will be reviewed.

Public Authority (Including full address)	Blackpool Council Enter full postal address		
Name of applicant	Details of the person completing the form	Directorate	
Full Address	Provide the full postal address of your Directorate		
Contact Details	Provide full contact details, including email address. Make it easy for the Line Manager, or anyone else associated with the process to contact you.		
Investigation/ Operation Name	This may be an investigation reference number allocated to this case, or some other reference.		
Investigating Officer (if a person other than the applicant)	If someone who is not the investigator is completing the form, then the investigators details must be put in this box.		

Unique Reference Number	To be allocated by Democratic Governance
--------------------------------	--

Details of the Application

1. Give job title of Line Manager in accordance with Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 No. 521

The exact position of the Line Manager should be given e.g. Chief Internal Auditor.

2. Describe the purpose of the specific operation of investigation.

Describe the investigation to date including the offences and the relevant legislation. When, where and how are the offences occurring. Remember the Line Manager needs to be clear what the offence is and the circumstances (keep information relevant and to the point).

Include the details of the suspects and persons involved and the role they play within the investigation. (Do not put confidential information in such as informants' names).

Consider disclosure implications under CPIA about not revealing unnecessary information. However, the Line Manager needs sufficient relevant information to make a decision. The provisions of using CPIA sensitive information may be a way of dealing with the sensitivity issues later, by editing material if it has to be disclosed. However, if the document contains sensitive information remember to keep it secure at all times.

Cross-reference where necessary to other relevant applications.

Refer to the evaluation of the intelligence, as the Authorising Office should consider its provenance and value.

WHEN MENTIONING THE OFFENCE REMEMBER IT MUST BE AS PER BOX 6

3. Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, recorder) that may be used.

This should be completed, after attending the area of where the activity is to be carried out. A surveillance assessment should be completed, taking into account risks or limiting factors. (Limiting factors are anything that can affect the success of the operation).

Consider the Line Manager statement in Box 12, the five Who, What, Where, When, Why and How? The applicant can only do what is authorised by the Line Manager, not what they have applied for.

Unique Reference Number	To be allocated by Democratic Governance
--------------------------------	--

Consider the aims and objective, confirmation of address may only need static observations, however lifestyle intelligence may require foot/mobile and use of covert cameras etc.

What exactly do you want to do? Is it static observations, foot or mobile? Do you want a combination? However, only ask for what you can realistically carry out. It is not a wish list, it should be carried out to achieve the objectives.

How do you want to carry out the surveillance and what equipment do you want to use? You must make the Line Manager aware of the capabilities of any equipment you want to use.

Where is the activity to take place? Who is the activity against and when do you want to carry it out?

What is the expected duration? It does not mean that it must only be authorised to this point. Once signed, the authorisation last for a three-month period. You must update the Line Manager when they set the review dates. If your operation ends prior to any review date or the three-month period, you must cancel it straight away and submit the cancellation form (RIP 3). It does not expire.

THIS IS NOT A WISH LIST, IT SHOULD BE THOUGHT THROUGH

REMEMBER YOU CAN ONLY DO WHAT IS AUTHORISED ON THE AUTHORISING SECTION, NOT WHAT YOU HAVE APPLIED FOR IN THIS SECTION.

4. The identities, where known, of those to be subject of the surveillance.

- **Name**
- **Address:**
- **DOB:**
- **Other information as appropriate**

If you do not know who the subjects are, insert any description you may have. If as a result of the surveillance, you identify anyone, you must submit this information on a review form to the Line Manager.

Consider any known associates. If the intelligence is that the subject of the surveillance has known associates, are they likely to become subjects of the surveillance? If so, detail them as part of the application.

Unique Reference Number	To be allocated by Democratic Governance
--------------------------------	--

5. Explain the information that is desired to obtain as a result of the surveillance.

These are the surveillance objectives. They should have been identified during the planning stage and a feasibility study carried out to assess whether they can be achieved. It is no use setting objective that cannot be achieved.

- What is the surveillance going to tell you?
- What, if any, criminality will it establish?
- Will it identify subjects involved in criminality?
- Will it house subject or their criminal associates?

Example:

- Identify the location of the subject’s place of work
- To gather information and evidence to establish the extent of the criminality
- Identify other persons involved, such as suppliers
- Identify other premises involved, such as storage buildings
- Obtain best evidence with photographic equipment to assist with identifying the offenders.

Obtain best evidence to assist with a prosecution of offenders.

6. Identify on which grounds the surveillance is necessary and proportionate .

Ensure that you know which grounds you are entitled to rely on:

- In the interests of national security;
- For the purpose of preventing or detecting crime or of preventing disorder;
- In the interests of public safety;
- For the purpose of protecting public health
- For the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department.

Due to the nature of the offence, if any other area above is applicable such as protection of public health, this should be made clear in the body of the application and the proportionality section.

You need to explain what other interventions/ tactics have been employed to resolve the issue(s) and the results.

Useful Examples are:

- Passing observations e.g. Police or Council employee
- Door Knocks
- Social Media enquiry
- Community Liaison
- Partner Intel Checks
- Internal Intel Checks

Why is it necessary at this stage of the enquiry to carry out activity?

What is the purpose of the operation?

How will the activity assist or progress the investigation?

What are the consequences of the proposed action?

Why do we need this evidence/ intelligence/ information?

Consequences of not taking action?

7. Describe precautions you will take to prevent/ minimise collateral intrusion.

(RIPA - Code paragraphs 3.8 to 3.11).

There are three parts to this section. You must answer them all, as this section directly impacts upon the proportionality test.

1. Ensure prevention and minimisation of Collateral Intrusion

- Visit the location of where the activity is to take place and carry out a risk assessment. (Who lives at the property that you may be watching? Have they got children who might be affected such as going to school?).
- Determine where you need to be carrying out the surveillance. (What else can you see?).
- What equipment will you be using and what will it see and record?
- Where will the cameras observe. (Public/ Private? Consider the position?).
- Types of recordings. (Photo's/ videos/ audio. Is it necessary?).
- Consider confidential information. It may be useful to paint the picture in words of what it is you will be watching in the locality. This will assist the Line Manager. You may also want to refer to any plans or maps attached to the application.

Unique Reference Number	To be allocated by Democratic Governance
--------------------------------	--

2. Why is the intrusion unavoidable?

Consider why the intrusion is unavoidable, such as the location and time frame that the observations have to be carried out. It may be that you are limited to the use of certain equipment only and therefore governed by its operating capabilities. Your observation position may be the only place you can use.

3. Manage any recordings obtained

In line with the Council' Policy any recordings need to be evidential, if not they should be destroyed using an appropriate manner e.g. shredding/ deleting after a maximum of 30 days. If the information obtained is deemed evidential then it must be stored securely and in accordance with Council's retention policy.

When evidential information is obtained e.g. video evidence, it is suggested that one master copy is sealed and retained by a Document Controller, should there be a legal challenge. Two further workings copies are also made

8. Line Manager's Statement.

Having read the application I am confident that the applicant has demonstrated that the surveillance is necessary, proportionate and justified and hereby authorise surveillance as detailed in the application.

If not authorising:

Having read the application I am NOT confident that the applicant has demonstrated that the surveillance is necessary, proportionate and justified and hereby DO NOT authorise surveillance as detailed in the application.

Remember that each case has to be assessed on its own merits

Name (print)		Job Title	
Signature		Date and Time	

9. Date of First Review	The Line Manager must set the review date. Consider what the applicant has stated regarding the length of time required. Remember, this is so you as the Line Manager can now review the need for the activity to continue on the date you have set.
--------------------------------	--

Appendix 5

CHIS 1 – AUTHORISATION (AIDE MEMOIRE)

PART II OF THE REGULATION OF INVESTIGATORY POWERS ACT (RIPA) 2000 APPLICATION FOR AUTHORISATION OF THE CONDUCT OR USE OF A COVERT HUMAN INTELLIGENCE SOURCE (CHIS)

Public Authority (Including full address)	Blackpool Council Enter full postal address
---	--

Name of applicant	Details of the person completing the form	Directorate	
--------------------------	---	--------------------	--

How will the source be referred to (i.e. what will be his/ her pseudonym or reference number)?	
What is the name and position of the person within the relevant investigating authority who will have day to day responsibility for dealing with the source, including the source's security and welfare (often referred to as the Handler)? Investigating Officer (if a person other than the applicant)	
What is the name or position of another person within the relevant investigating authority who will have general oversight of the use made of the source (often referred to as the Controller)?	
Who will be responsible for retaining (in secure, strictly controlled conditions, with need-to-know access) the source's true identity, a record of the use made of the source and the particulars required under RIP (Source Records) Regulations 2000 (SI 2000/2725)?	
Investigation/Operation Name (if applicable)	

DETAILS OF APPLICATION

1. Give the position of the Authorising Officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 No. 521.

2. Describe the purpose of the specific operation or investigation

3. Describe in detail the purpose for which the source will be tasked or used

4. Describe in detail the proposed covert conduct of the source or how the source is to be used.

5. Identify on which grounds the conduct or the use of the source is necessary under Section 29(3) of RIPA. (*Delete those that are inapplicable. Ensure that you know which of these grounds you are entitled to rely on (eg. SI 2010 No.521).*)

- In the interests of national security;
- For the purpose of preventing or detecting crime or of preventing disorder;
- In the interests of the economic well-being of the United Kingdom;
- In the interests of public safety;
- for the purpose of protecting public health;
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department.

<p>6. Explain <u>why</u> this conduct or use of the source is necessary on the grounds you have identified</p>
<p>Code paragraph 3.2</p>
<p>7. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. Describe precautions you will take to minimise collateral intrusion and how any will be managed.</p>
<p>Code paragraphs 3.8 to 3.11</p>
<p>8. Are there any particular sensitivities in the local community where the source is to be used? Are similar activities being undertaken by other public authorities that could impact on the deployment of the source)?</p>
<p>Code paragraphs 3.17 to 3.18</p>
<p>9. Provide an assessment of the risk to the source in carrying out the proposed conduct</p>
<p>Code paragraph 6.14</p>
<p>10. Explain why this conduct or use of the source is proportionate to what it seeks to achieve. How intrusive might it be on the subject(s) of surveillance or on others? How is this intrusion outweighed by the need for a source in operational terms, and could the evidence be obtained by any other means?</p>
<p>Code paragraphs 3.3 to 3.5</p>

11. Indicate the likelihood of acquiring any Confidential Information.

Code paragraphs 4.1 to 4.21.

References for any other linked authorisations:

12. Applicant's Details.

Name (print)		Grade/Position	
Signature		Tel No:	
Date			

13. Authorising Officer's Statement

Spell out the "5 Ws" – Who; What; Where; When; Why and HOW

The authorisation should identify the pseudonym or reference number of the source, not the true identity.

14. Explain why you believe the conduct or use of the source is necessary and why you believe the conduct or use of the source to be proportionate to what is sought to be achieved by their engagement?

Code paragraph 3.2

Code paragraphs 3.3 to 3.5

15. Confidential Information Authorisation. Supply details demonstrating compliance with

Code paragraphs 4.1 to 4.21

16. Date of first review:			
17. Programme for subsequent reviews of this authorisation			
<p>Only complete this box if review dates after first review are known. If not, or inappropriate to set additional review dates, then leave blank.</p> <p>Code paragraphs 5.15 and 5.16</p>			
18. Authorising Officer's Details			
Name (print)		Grade/Position	
Signature		Time and date granted Time and date authorisation ends	Remember, an authorisation must be granted for a 12 month period.
Date			
19. Urgent Authorisation			
<p>Code paragraphs 5.13 and 5.14</p> <p>Explain why you considered the case so urgent that an oral instead of a written authorisation was given.</p>			
20. If you are entitled to act only in urgent cases: explain why it was not reasonably practicable for the application to be considered by a fully designated Authorising Officer			
21. Authorising Officer of urgent authorisation			
Name (print)		Grade/Position	
Signature		Date and Time	
Urgent authorisation expiry date:		Expiry time:	

Remember the 72-hour rule for urgent authorisations – check Code of Practice [Code Paragraph 5.14].

Unique Reference Number	To be allocated by Democratic Governance
--------------------------------	--

CHIS 2 – CANCELLATION (AIDE MEMOIRE)

PART II OF THE REGULATION OF INVESTIGATORY POWERS ACT (RIPA) 2000 CANCELLATION OF AN AUTHORISATION FOR THE USE OR CONDUCT OF A COVERT HUMAN INTELLIGENCE SOURCE (CHIS)

Public Authority (Including full address)	Blackpool Council Enter full postal address
---	--

Name of applicant	Details of the person completing the form	Directorate	
Full Address	Provide the full postal address of your Directorate		
Contact Details	Provide full contact details, including email address. Make it easy for the Authorising Officer, or anyone else associated with the process to contact you.		
Investigation/ Operation Name	This may be an investigation reference number allocated to this case, or some other reference.		

Details of the Cancellation

1. Explain the reason(s) for the cancellation of the authorisation:

Unique Reference Number	To be allocated by Democratic Governance
--------------------------------	--

2. Explain the value of the source in the operation:			
This should identify the pseudonym or reference number of the source, not the true identity.			
3. Authorising officer's statement			
I, _____ hereby authorise the cancellation of the use or conduct of the source as detailed above.			
Effective Date		Effective Time	
Name (print)		Grade/Position	
Signature		Date	

Unique Reference Number	To be allocated by Democratic Governance
--------------------------------	--

CHIS 3 – RENEWAL (AIDE MEMOIRE)

**PART II OF THE REGULATION OF INVESTIGATORY POWERS ACT (RIPA) 2000
APPLICATION FOR RENEWAL OF A COVERT HUMAN INTELLIGENCE SOURCE (CHIS)
AUTHORISATION
(Please see the original authorisation)**

Public Authority (Including full address)	Blackpool Council Enter full postal address
---	--

Name of applicant	Details of the person completing the form	Directorate	
Full Address	Provide the full postal address of your Directorate		
Contact Details	Provide full contact details, including email address. Make it easy for the Authorising Officer, or anyone else associated with the process to contact you.		
Pseudonym or reference number of source			
Investigation/ Operation Name	This may be an investigation reference number allocated to this case, or some other reference.		
Renewal Number			

Details of the Renewal

1. Renewal numbers and dates of any previous renewals.	
Renewal Number	Date

Unique Reference Number	To be allocated by Democratic Governance
--------------------------------	--

2. Detail any significant changes to the information as listed in the original authorisation as it applies at the time of the renewal.
3. Detail why it is necessary to continue with the authorisation, including details of any tasking given to the source.
4. Detail why the use or conduct of the source is still proportionate to what it seeks to achieve.
5. Detail the use made of the source in the period since the grant of authorisation or, as the case may be, latest renewal of the authorisation.
6. List the tasks given to the source during that period and the information obtained from the conduct or use of the source.
7. Detail the results of regular reviews of the use of the source.
8. Give details of the review of the risk assessment on the security and welfare of using the

Unique Reference Number	To be allocated by Democratic Governance
--------------------------------	--

source.

9. Applicants Details			
Name (print)		Telephone number:	
Grade/Rank:		Date:	
Signature:			

10. Authorising Officer's comments
<p>This box must be completed.</p>

11. Authorising Officer's Statement
<p>I, _____, hereby authorise the renewal of the conduct/ use of the source as detailed above. The renewal of this authorisation will last for 12 months unless further renewed writing.</p> <p>This authorisation will be reviewed frequently to assess the need for the authorisation to continue.</p> <p>The authorisation should identify the pseudonym or reference number of the source and not the true identify.</p>

Name (print)		Grade/Position:	
Signature:		Date:	
Renewal from:		Time:	
End of Authorisation Date:		Time:	

Unique Reference Number

To be allocated by Democratic Governance
--

--	--	--	--

Date of first review:	
Date of subsequent reviews of this authorisation:	

Unique Reference Number	To be allocated by Democratic Governance
--------------------------------	--

CHIS 4 – REVIEW (AIDE MEMOIRE)

PART II OF THE REGULATION OF INVESTIGATORY POWERS ACT (RIPA) 2000 REVIEW OF A COVERT HUMAN INTELLIGENCE SOURCE (CHIS) AUTHORISATION

Public Authority (Including full address)	Blackpool Council Enter full postal address
---	--

Name of applicant	Details of the person completing the form	Directorate	
Full Address	Provide the full postal address of your Directorate		
Contact Details	Provide full contact details, including email address. Make it easy for the Authorising Officer, or anyone else associated with the process to contact you.		
Pseudonym or reference number of source			
Operation Name			
Date of authorisation or last renewal		Expiry date of authorisation or last renewal	
Review Number			

Details of the Review

1. Review number and dates of any previous reviews.	
Review Number	Date

Unique Reference Number	To be allocated by Democratic Governance
--------------------------------	--

2. Summary of the investigation/operation to date, including what information has been obtained and the value of the information so far obtained.
3. Detail the reasons why it is necessary to continue using a Covert Human Intelligence Source.
4. Explain how the proposed activity is still proportionate to what it seeks to achieve.
5. Detail any incidents of collateral intrusion and the likelihood of any further incidents of collateral intrusions occurring.
6. Give details of any confidential information acquired or accessed and the likelihood of acquiring confidential information.
7. Give details of the review of the risk assessment on the security and welfare of using the source.

8. Applicants Details			
Name (print)		Telephone number:	

Unique Reference Number	To be allocated by Democratic Governance
--------------------------------	--

Grade/Position:		Date:	
Signature:			

9. Review Officer's Comments, including whether or not the use or conduct of the source should continue?

--

10. Authorising Officer's Statement

I, _____, hereby agree that the use or conduct as detailed above should/ not continue until its next review/ renewal (it should be cancelled immediately).

The authorisation should identify the pseudonym or reference number of the source, not the identity.

Name (print)		Grade/Position:	
Signature		Date:	

11. Date of next Review	
--------------------------------	--

Appendix 6

Authorised Officers			
Name	Job Title	Email Address	Telephone Number
Neil Jack	Chief Executive	neil.jack@blackpool.gov.uk	(01253) 477000
Tim Coglan	Service Manager – Public Protection	tim.coglan@blackpool.gov.uk	(01253) 478376
Tracy Greenhalgh	Chief Internal Auditor	tracy.greenhalgh@blackpool.gov.uk	(01253) 478554
Glen Phoenix	Trading Standards Manager (Enforcement)	glen.phoenix@blackpool.gov.uk	(01253) 478381
Steve Thompson	Director of Resources	Steve.thompson@blackpool.gov.uk	(01253) 478505

Appendix 7

APPLICATION FOR JUDICIAL APPROVAL FOR AUTHORISATION TO OBTAIN OR DISCLOSE COMMUNICATIONS DATA, TO USE A COVERT HUMAN INTELLIGENCE SOURCE OR TO CONDUCT DIRECTED SURVEILLANCE. REGULATION OF INVESTIGATORY POWERS ACT 2000 SECTIONS 23A, 23B, 32A, 32B.

Local authority	
Local authority department	
Offence under investigation	
Address of premises or identity of subject	

Covert technique requested: (tick one and specify details)

Communications Data

Covert Human Intelligence Source

Directed Surveillance

Summary of details

Note: this application should be read in conjunction with the attached RIPA authorisation/ RIPA application or notice.

Investigating Officer	
Authorising Officer/Designated Person	
Officer(s) appearing before JP	
Address of applicant department	
Contact telephone number	
Contact email address (optional)	
Local authority reference	
Number of pages	

Public Authority (Including full address)	Blackpool Council Enter full postal address		
Name of applicant	Details of the person completing the form	Directorate	
Full Address	Provide the full postal address of your Directorate		
Contact Details	Provide full contact details, including email address. Make it easy for the Authorising Officer, or anyone else associated with the process to contact you.		
Operation Name			
Date of authorisation or last renewal		Expiry date of authorisation or last renewal	
Review Number			

Details of the Review

1. Review number and dates of any previous reviews.	
Review Number	Date

2. Summary of the investigation/operation to date, including what information has been obtained and the value of the information so far obtained.

3. Detail the reasons why it is necessary to continue using Direct Surveillance.
4. Explain how the proposed activity is still proportionate to what it seeks to achieve.
5. Detail any incidents of collateral intrusion and the likelihood of any further incidents of collateral intrusions occurring.
6. Give details of any confidential information acquired or accessed and the likelihood of acquiring confidential information.

7. Applicants Details			
Name (print)		Telephone number:	
Grade/Position:		Date:	
Signature:			

8. Review Officer's Comments, including whether or not the use or conduct of the source should continue?
9. Authorising Officer's Statement

Blackpool Council

I, _____, hereby agree that the directed surveillance investigation/operation as detailed above [should/should not] continue [until its next review/renewal][it should be cancelled immediately].

Name (print)		Grade/Position:	
Signature		Date:	

10. Date of next Review	
--------------------------------	--

Appendix 8

Protection of Freedoms Act 2012 – changes to provisions under the Regulation of Investigatory Powers Act 2000 (RIPA)

Home Office guidance to local
authorities in England and Wales
on the judicial approval process for
RIPA and the crime threshold for
directed surveillance



Home Office

October 2012

Contents

1. Introduction: how the law has changed.....	5
2. Local Authority use of RIPA.....	6
The existing regulatory framework.....	6
The techniques which local authorities may use.....	6
Rank of local authority authorising officers/designated persons.....	7
Time limits.....	7
3. Directed surveillance crime threshold.....	8
Impact on investigations.....	8
4. Judicial approval.....	10
What the changes mean for local authorities.....	10
Procedure for applying for judicial approval.....	10
-Making the application.....	10
-Arranging a hearing.....	11
-Attending a hearing.....	12
-Decision.....	12
-Outcomes.....	13
-Complaints/Judicial Review.....	14
5. Other sources of reference.....	15
6. Home Office point of contact.....	16
Annex A:	
Flowchart – Local Authority procedure: application to a justice of the peace Seeking an order to approve the grant of a RIPA authorisation or notice.....	17
Annex B:	
Judicial application/order form.....	18
Annex C:	
Communications data RIPA authorisations or notices.....	20

1. INTRODUCTION: HOW THE LAW HAS CHANGED

1. On 1 November 2012 two significant changes will take effect governing how local authorities use RIPA.
 - **Approval of Local Authority Authorisations under RIPA by a Justice of the Peace:** The amendments in the Protection of Freedoms Act 2012¹ will mean that local authority authorisations and notices under RIPA for the use of particular covert techniques can only be given effect once an order approving the authorisation or notice has been granted by a Justice of the Peace (JP).
 - **Directed surveillance crime threshold:** Amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (“the 2010 Order”)² mean that a local authority can now only grant an authorisation under RIPA for the use of directed surveillance where the local authority is investigating particular types of criminal offences. These are criminal offences which attract a maximum custodial sentence of six months or more or criminal offences relating to the underage sale of alcohol or tobacco.
2. This guidance is non-statutory but provides advice on how local authorities can best approach these changes in law and the new arrangements that need to be put in place to implement them effectively. It is supplementary to the legislation and to the statutory Codes of Practice. If a local authority has any doubts about the new regime they should consult their legal advisers. This guidance is intended for local authority investigation teams that may use covert techniques, including Trading Standards, Environmental Health and Benefit Fraud Officers. However, it will also be of use to authorising officers and designated persons and to those who oversee the use of investigatory techniques in local authorities including elected members.
3. Separate guidance is available for Magistrates’ Courts in England and Wales and local authorities in Scotland.

¹ Sections 37 and 38 of the Protection of Freedoms Act 2012 amend RIPA and will come into force on 1 November 2012.

² The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 [SI 2010/521] will be amended by the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 [SI 2012/1500] on 1 November 2012. See Section 5 for link

2. LOCAL AUTHORITY USE OF RIPA

THE EXISTING REGULATORY FRAMEWORK

4. RIPA sets out a regulatory framework for the use of covert investigatory techniques by public authorities. RIPA does not provide any powers to carry out covert activities. If such activities are conducted by council officers, then RIPA regulates them in a manner that is compatible with the European Convention on Human Rights (ECHR), particularly Article 8, the right to respect for private and family life.
5. RIPA limits local authorities to using three covert techniques (details set out below) for the purpose of preventing or detecting crime or preventing disorder.
6. Use of these techniques has to be authorised internally by an authorising officer or a designated person. They can only be used where it is considered necessary (e.g. to investigate a suspected crime or disorder) and proportionate (e.g. balancing the seriousness of the intrusion into privacy against the seriousness of the offence and whether the information can be obtained by other means). The relevant Codes of Practice should be referred to for further information on the scope of powers, necessity and proportionality.³

THE TECHNIQUES WHICH LOCAL AUTHORITIES MAY USE

7. **Directed surveillance** is essentially covert surveillance in places other than residential premises or private vehicles⁴.
8. Local authorities cannot conduct 'intrusive' surveillance (i.e. covert surveillance carried out in residential premises or private vehicles⁵) under the RIPA framework.
9. A **covert human intelligence source (CHIS) includes** undercover officers, public informants and people who make test purchases.
10. **Communications data (CD)** is the 'who', 'when' and 'where' of a communication, but not the 'what' (i.e. the content of what was said or written). RIPA groups CD into three types:
 - 'traffic data' (which includes information about where the communications are made or received);
 - 'service use information' (such as the type of communication, time sent and its duration); and
 - 'subscriber information' (which includes billing information such as the name, address and bank details of the subscriber of telephone or internet services).
11. Under RIPA a local authority can only authorise the acquisition of the less intrusive types of CD: service use and subscriber information. Under **no circumstances** can local authorities be authorised to obtain traffic data under RIPA.
12. Local authorities are **not** permitted to intercept the content of any person's communications and it is an offence to do so without lawful authority.

3 See section 5 for links to the relevant legislation and codes of practice.

4 Further information on directed surveillance can be found in the Covert Surveillance and Property Interference Code of Practice.

5 Places where legal consultations are likely to take place will also be treated as intrusive surveillance.

RANK OF LOCAL AUTHORITY AUTHORISING OFFICERS/DESIGNATED PERSONS

13. Local authority authorising officers/designated persons will remain as designated by RIPA consolidating orders SI 2010 Nos.480 and 521:
 - Director, Head of Service, Service Manager⁶ or equivalent.
14. The authorisation of directed surveillance or use of a CHIS likely to obtain confidential information or the deployment of a juvenile or vulnerable person (by virtue of mental or other condition) as a CHIS requires authorisation by the most senior local authority officer – Head of Paid Service or, in his/her absence, the acting Head of Paid Service.
15. If there is any doubt regarding sufficiency of rank you should contact your Local Authority Monitoring Officer who will be able to advise you.

TIME LIMITS

16. The current time limits for an authorisation or notice will continue⁷. That is: 3 months for directed surveillance and 12 months for a CHIS (1 month if the CHIS is 18). Authorisations and notices for CD will be valid for a maximum of one month from the date the JP has approved the grant. This means that the conduct authorised should have been commenced or the notice served within that month.
17. A renewal must be authorised prior to the expiry of the original authorisation, but it runs from the expiry date and time of that original authorisation. Authorisations may be renewed more than once if still considered necessary and proportionate and approved by the JP.
18. Applications for renewals should not be made until shortly before the original authorisation period is due to expire but local authorities must take account of factors which may delay the renewal process (e.g. intervening weekends or the availability of the relevant local authority authorising officer and a JP to consider the application).

⁶ For CD RIPA applications, the Local Government Group and the Interception of Communications Commissioner's Office have advised that a Principal Trading Standards Officer is not considered to be of sufficient seniority to act as the Designated Person.

⁷ See section 43 RIPA.

3. DIRECTED SURVEILLANCE CRIME THRESHOLD

19. The crime threshold applies only to the authorisation of **directed surveillance** by local authorities under RIPA, not to the authorisation of local authority use of CHIS or their acquisition of CD. The threshold will come into effect on 1 November 2012.
20. The amendments to the 2010 Order have the following effect:
 - Local authorities can only authorise use of directed surveillance under RIPA to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment **or** are related to the underage sale of alcohol and tobacco. The offences relating to the latter are in article 7A of the 2010 Order⁸.
 - Local authorities **cannot** authorise directed surveillance for the purpose of preventing disorder unless this involves a criminal offence(s) punishable (whether on summary conviction or indictment) by a maximum term of at least 6 months' imprisonment.
 - Local authorities may therefore continue to authorise use of directed surveillance in more serious cases as long as the other tests are met – i.e. that it is necessary and proportionate and where prior approval from a JP has been granted. Examples of cases where the offence being investigated attracts a maximum custodial sentence of six months or more could include more serious criminal damage, dangerous waste dumping and serious or serial benefit fraud.
 - Local authorities may also continue to authorise the use of directed surveillance for the purpose of preventing or detecting specified criminal offences relating to the underage sale of alcohol and tobacco where the necessity and proportionality test is met and prior approval from a JP has been granted.
 - A local authority **may not authorise** the use of directed surveillance under RIPA to investigate disorder that does not involve criminal offences or to investigate low-level offences which may include, for example, littering, dog control and fly-posting.
21. The change will affect authorisations or renewals which are granted on or after 1 November. It will not affect authorisations or renewals granted before that date.

IMPACT ON INVESTIGATIONS

22. At the start of an investigation, council officers will need to satisfy themselves that what they are investigating is a criminal offence. Directed surveillance is an invasive technique and at the point it is decided whether or not to authorise its use it must be clear that the threshold is met and that it is necessary and proportionate to use it.
23. During the course of an investigation the type and seriousness of offences may change. The option of authorising directed surveillance is dependent on the offence under investigation attracting a sentence of a maximum six months imprisonment or more or being related to the underage sale of alcohol and tobacco. Providing the offence under investigation is one which appears on the statute book with at least a maximum six months term of imprisonment or is related to the specific offences listed in the order concerning the underage sale of alcohol and tobacco an application can be made. However, if during the investigation it becomes clear that the activity being investigated does not amount to a criminal offence or that it would be a less serious offence that does not meet the threshold the use of directed surveillance should cease. If a directed surveillance authorisation is already in force it should be cancelled.

⁸ See section 5 for links to the relevant legislation

24. Directed surveillance will be authorised against a specific offence which meets the threshold, and the type and the timing of the deployment of the surveillance will always reflect this. There may be cases where it is possible, with the same evidence obtained by the same deployment, to substantiate a variety of different charges, some of which fall below the threshold, it will be for the courts to decide whether to admit – and what weight to attach to – the evidence obtained in the lesser charges.
25. Local authorities will no longer be able to use directed surveillance in some cases where it was previously authorised. But this does not mean that it will not be possible to investigate these areas with a view to stopping offending behaviour. The statutory RIPA Code of Practice on covert surveillance makes it clear that routine patrols, observation at trouble ‘hotspots’, immediate response to events and overt use of CCTV are all techniques which do not require RIPA authorisation.⁹

⁹ See paragraphs 2.21-2.29 of the Covert Surveillance and Property Interference Code of Practice.

4. JUDICIAL APPROVAL

WHAT THE CHANGES MEAN FOR LOCAL AUTHORITIES

26. From 1 November 2012, sections 37 and 38 of the Protection of Freedoms Act 2012 will commence. This will mean that a local authority who wishes to authorise the use of directed surveillance, acquisition of CD and use of a CHIS under RIPA will need to obtain an order approving the grant or renewal of an authorisation or notice from a JP (a District Judge or lay magistrate) before it can take effect. If the JP is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate he/she will issue an order approving the grant or renewal for the use of the technique as described in the application.
27. The new judicial approval mechanism is in addition to the existing authorisation process under the relevant parts of RIPA as outlined in the Codes of Practice. The current local authority process of assessing necessity and proportionality, completing the RIPA authorisation/application form and seeking approval from an authorising officer/designated person will remain the same.
28. The inspection regimes of the independent RIPA oversight Commissioners will continue to apply to local authorities and the frequency and nature of their independent inspections of local authorities is not expected to change.
29. The judiciary is independent and it is not the role of the Commissioners to inspect the decision of the JP.¹⁰ However the Commissioners will continue to have an important oversight role and will continue to inspect local authority use of RIPA. If the Commissioners identify an error in the authorisation process they will, as now, need to consider the best course of action. This may include asking the local authority to cancel the authorisation in question and, if appropriate, complete a new authorisation addressing their concerns which will need to be approved by the JP in the usual way. When an error is brought to the attention of a local authority they should cease the activity authorised.
30. The Commissioners will continue to advise local authorities of the procedures and training to adopt, on what is best practice and will continue to report to Parliament on relevant trends and findings.

PROCEDURE FOR APPLYING FOR JUDICIAL APPROVAL

Making the Application

31. The flowchart at Annex A outlines the procedure for applying for judicial approval. The application must be made by the public authority that has granted the authorisation¹¹. Following approval by the authorising officer/designated person the first stage of the process is for the local authority to contact Her Majesty's Courts and Tribunals Service (HMCTS) administration team at the magistrates' court to arrange a hearing.

¹⁰ See section 62(2A) RIPA.

¹¹ Some local authorities may enter into arrangements to form a regional group with other local authorities but the group cannot itself make the application. Only local authority officers in local authorities described in SIs 2010 Nos.480 and 521 are able to authorise under RIPA.

32. The local authority will provide the JP with a copy of the original RIPA authorisation or notice and the supporting documents setting out the case. This forms the basis of the application to the JP and **should contain all information that is relied upon**. For communications data requests the RIPA authorisation or notice may seek to acquire consequential acquisition of specific subscriber information. The necessity and proportionality of acquiring consequential acquisition will be assessed by the JP as part of his consideration (see Annex C for considerations relating to CD authorisations and notices).
33. The original RIPA authorisation or notice should be shown to the JP but will be retained by the local authority so that it is available for inspection by the Commissioners' offices and in the event of any legal challenge or investigations by the Investigatory Powers Tribunal (IPT). The court may wish to take a copy.
34. In addition, the local authority will provide the JP with a partially completed judicial application/order form (at Annex B).
35. Although the local authority is required to provide a brief summary of the circumstances of the case on the judicial application form, this is supplementary to and does not replace the need to supply the original RIPA authorisation as well.
36. The order section of this form will be completed by the JP and will be the official record of the JP's decision. The local authority will need to obtain judicial approval for all initial RIPA authorisations/ applications **and renewals** and the local authority will need to retain a copy of the judicial application/ order form after it has been signed by the JP. There is no requirement for the JP to consider either cancellations or internal reviews.

Arranging a Hearing

37. It will be important for each local authority to establish contact with HMCTS administration at the magistrates' court. HMCTS administration will be the first point of contact for the local authority when seeking a JP approval. The local authority will inform HMCTS administration as soon as possible to request a hearing.
38. On the rare occasions where out of hours access to a JP is required then it will be for the local authority to make local arrangements with the relevant HMCTS legal staff. In these cases the local authority will need to provide two partially completed judicial application/order forms so that one can be retained by the JP. The local authority should provide the court with a copy of the signed judicial application/order form the next working day.
39. In most emergency situations where the police have power to act, then they are able to authorise activity under RIPA without prior JP approval. No RIPA authority is required in immediate response to events or situations where it is not reasonably practicable to obtain it (for instance when criminal activity is observed during routine duties and officers conceal themselves to observe what is happening).
40. Where renewals are timetabled to fall outside of court hours, for example during a holiday period, it is the local authority's responsibility to ensure that the renewal is completed ahead of the deadline. Out of hours procedures are for emergencies and should not be used because a renewal has not been processed in time.

Attending a Hearing

41. The hearing is a 'legal proceeding' and therefore local authority officers need to be formally designated to appear, be sworn in and present evidence or provide information as required by the JP.
42. The hearing will be in private and heard by a single JP who will read and consider the RIPA authorisation or notice and the judicial application/order form. He/she may have questions to clarify points or require additional reassurance on particular matters.
43. Local authorities will want to consider who is best able to answer the JP's questions on the policy and practice of conducting covert operations and detail of the case itself. It is envisaged that the case investigator will be able to fulfil this role. The investigator will know the most about the investigation and will have determined that use of a covert technique is required in order to progress a particular case. The local authority may consider it appropriate for the SPoC (single point of contact) to attend for applications for CD RIPA authorisations or notices (see Annex C for considerations relating to CD authorisations and notices). This does not, however, remove or reduce in any way the duty of the authorising officer to determine whether the tests of necessity and proportionality have been met. Similarly, it does not remove or reduce the need for the forms and supporting papers that the authorising officer has considered and which are provided to the JP to make the case (see paragraphs 47-48).
44. The usual procedure would be for local authority Standing Orders to designate certain officers, including SPoCs, for the purpose of presenting RIPA cases to JPs under section 223 of the Local Government Act 1972. A pool of suitable officers could be designated at the start of the year when the Orders are examined and adjusted as appropriate throughout the year.
45. It is not envisaged that the skills of legally trained personnel will be required to make the case to the JP and this would be likely to, unnecessarily, increase the costs of local authority applications.

Decision

46. The JP will consider whether he or she is satisfied that at the time the authorisation was granted or renewed or the notice was given or renewed, there were reasonable grounds for believing that the authorisation or notice was necessary and proportionate. They will also consider whether there continues to be reasonable grounds. In addition they must be satisfied that the person who granted the authorisation or gave the notice was an appropriate designated person within the local authority and the authorisation was made in accordance with any applicable legal restrictions, for example that the crime threshold for directed surveillance has been met.¹²

¹² Further information on these restrictions can be found in the Regulation of Investigatory Powers Act 2000: Consolidating Orders and Codes of Practice, SI 2012 No.1500 (The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment), SI 2000 No.2793 (The Regulation of Investigatory Powers (Juveniles) Order 2000) and the OSC Procedures and guidance manual, available to public authorities on request from the Office of Surveillance Commissioners.

47. **The forms and supporting papers must by themselves make the case. It is not sufficient for the local authority to provide oral evidence where this is not reflected or supported in the papers provided.** The JP may note on the form any additional information he or she has received during the course of the hearing but information fundamental to the case should not be submitted in this manner.
48. If more information is required to determine whether the authorisation or notice has met the tests then the JP will refuse the authorisation. If an application is refused the local authority should consider whether they can reapply, for example, if there was information to support the application which was available to the local authority, but not included in the papers provided at the hearing.
49. The JP will record his/her decision on the order section of the judicial application/order form. HMCTS administration will retain a copy of the local authority RIPA authorisation or notice and the judicial application/order form. This information will be retained securely. Magistrates' courts are not public authorities for the purposes of the Freedom of Information Act 2000.
50. The local authority will need to provide a copy of the order to the communications the SPoC (Single Point of Contact) for all CD requests. SPoCs must not acquire the CD requested, either via the CSP or automated systems until the JP has signed the order approving the grant.

Outcomes

51. Following their consideration of the case the JP will complete the order section of the judicial application/order form (see form at Annex B) recording their decision. The various outcomes are detailed below and reflected on the flowchart at Annex A.
52. The JP may decide to¹³ –

- **Approve the Grant or renewal of an authorisation or notice**

The grant or renewal of the RIPA authorisation or notice will then take effect and the local authority may proceed to use the technique in that particular case.

In relation to CD, the local authority will be responsible for providing a copy of the order to the SPoC.

- **Refuse to approve the grant or renewal of an authorisation or notice**

The RIPA authorisation or notice will not take effect and the local authority may **not** use the technique in that case.

Where an application has been refused the local authority may wish to consider the reasons for that refusal. For example, a technical error in the form may be remedied without the local authority going through the internal authorisation process again. The local authority may then wish to reapply for judicial approval once those steps have been taken.

¹³ See sections 23B(3) and 32B(3) of the Regulation of Investigatory Powers Act 2000.

- **Refuse to approve the grant or renewal and quash the authorisation or notice**

This applies where a magistrates' court refuses to approve the grant, giving or renewal of an authorisation or notice and decides to quash the original authorisation or notice.

The court must not exercise its power to quash that authorisation or notice unless the applicant has had at least 2 business days from the date of the refusal in which to make representations.

Complaints/Judicial Review

53. There is no complaint route for a judicial decision unless it was made in bad faith. Any complaints should be addressed to the Magistrates' Advisory Committee.
54. A local authority may only appeal a JP decision on a point of law by judicial review. If such a concern arises, the local authority should consult their legal advisers.
55. The IPT will continue to investigate complaints by individuals about the use of RIPA techniques by public bodies, including local authorities. If, following a complaint to them, the IPT does find fault with a RIPA authorisation or notice it has the power to quash the JP's order which approved the grant or renewal of the authorisation or notice.

5. OTHER SOURCES OF REFERENCE

- The Regulation of Investigatory Powers Act 2000
<http://www.legislation.gov.uk/ukpga/2000/23/contents>
- RIPA Explanatory Notes
<http://www.legislation.gov.uk/ukpga/2000/23/notes/contents>
- RIPA statutory codes of practice
 - Covert Surveillance and Property Interference
<http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa/forms/code-of-practice-covert>
 - Covert Human Intelligence Sources
<http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa/forms/code-of-practice-human-intel>
 - Acquisition & Disclosure of Communications Data
<http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa/forms/code-of-practice-acquisition>
- SI 2000 No.2793 (The Regulation of Investigatory Powers (Juveniles) Order 2000)
<http://www.legislation.gov.uk/uksi/2000/2793/made>
- SI 2010 No.480 – Regulation of Investigatory Powers (Communications Data) Order 2010
<http://www.legislation.gov.uk/uksi/2010/480/contents/made>
- SI 2010 N0.521 – Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010
<http://www.legislation.gov.uk/uksi/2010/9780111490365/contents>
- SI 2010 No.461 (The Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010)
<http://www.legislation.gov.uk/uksi/2010/461/contents/made>
- SI 2012 No.1500 (The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012)
<http://www.legislation.gov.uk/uksi/1500/contents>

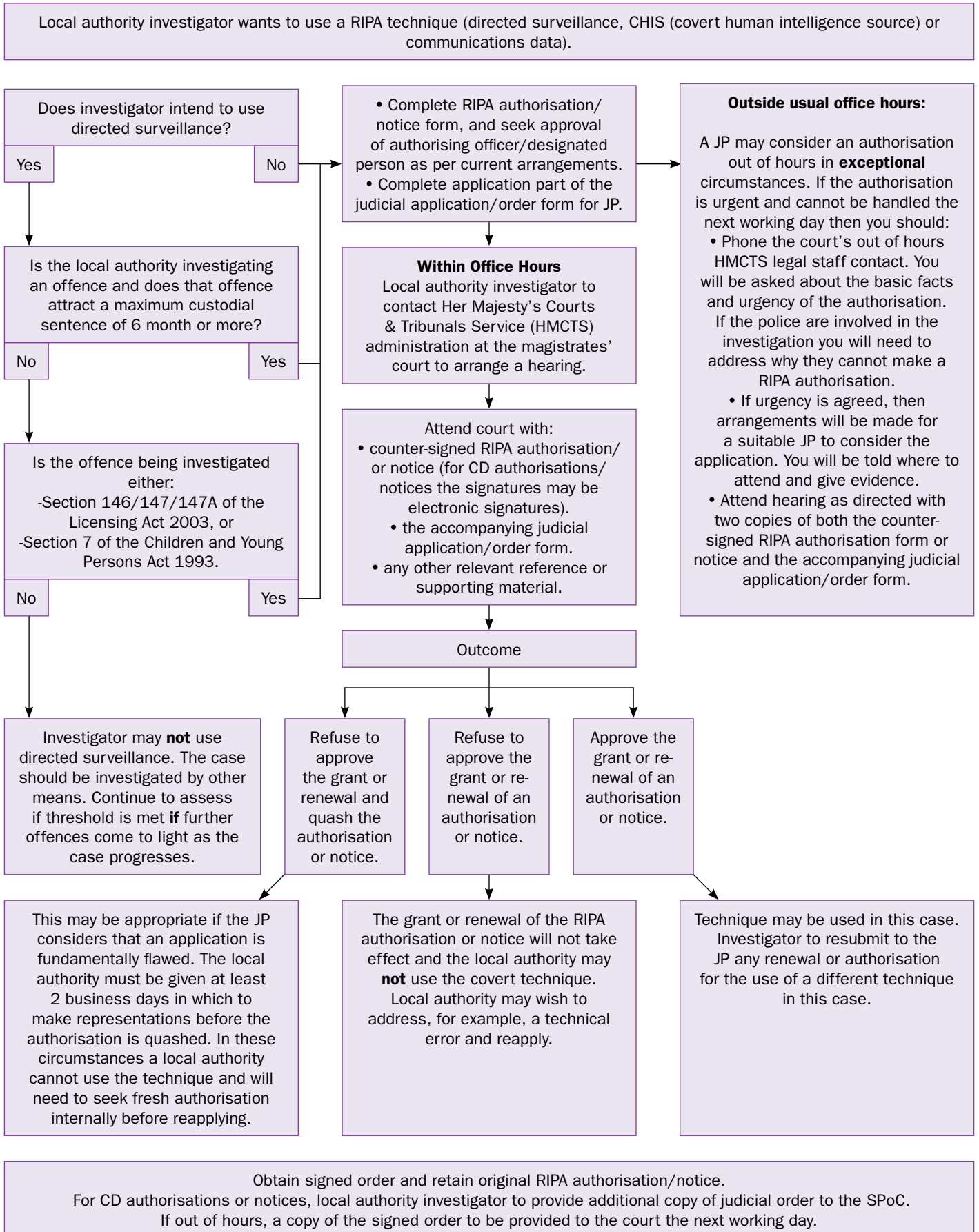
6. HOME OFFICE POINT OF CONTACT

Further information is available on request from:

RIPA Team
Home Office
5th Floor Peel Building
2 Marsham Street
London SW1P 4DF
Email: commsdata@homeoffice.x.gsi.gov.uk

ANNEX A

LOCAL AUTHORITY PROCEDURE: APPLICATION TO A JUSTICE OF THE PEACE SEEKING AN ORDER TO APPROVE THE GRANT OF A RIPA AUTHORISATION OR NOTICE



ANNEX B

Application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Local authority:.....

Local authority department:

Offence under investigation:.....

Address of premises or identity of subject:

.....

.....

Covert technique requested: (tick one and specify details)

Communications Data

Covert Human Intelligence Source

Directed Surveillance

Summary of details

.....

.....

.....

.....

.....

.....

Note: this application should be read in conjunction with the attached RIPA authorisation/RIPA application or notice.

Investigating Officer:.....

Authorising Officer/Designated Person:

Officer(s) appearing before JP:

Address of applicant department:.....

.....

Contact telephone number:.....

Contact email address (optional):

Local authority reference:

Number of pages:.....

Order made on an application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Magistrates' court:.....

Having considered the application, I (tick one):

- am satisfied that there are reasonable grounds for believing that the requirements of the Act were satisfied and remain satisfied, and that the relevant conditions are satisfied and I therefore approve the grant or renewal of the authorisation/notice.
- refuse to approve the grant or renewal of the authorisation/notice.
- refuse to approve the grant or renewal and quash the authorisation/notice.

Notes

.....
.....
.....
.....
.....

Reasons

.....
.....
.....
.....
.....
.....

Signed:

Date:

Time:

Full name:

Address of magistrates' court:

ANNEX C

COMMUNICATIONS DATA (CD) RIPA AUTHORISATIONS OR NOTICES

Single Point of Contact (SPoC)

1. For CD requests, a Single Point of Contact (SPoC) undertakes the practical facilitation with the communications service provider (CSP) in order to obtain the CD requested. They will have received training specifically to facilitate lawful acquisition of CD and effective co-operation between the local authority and communications service providers.
2. Local authorities unable to call upon the services of an accredited SPoC should not undertake the acquisition of CD.
3. For CD requests the Home Office envisages that the local authority may also choose to authorise, under section 223 of the Local Government Act, their SPoC in order that they may appear in front of the JP. In cases where the type of CD or its retrieval is technically complex and the JP wants to satisfy him/herself that the CD sought meets the test, then the SPoC may be best placed to explain the technical aspects.
4. Following the hearing the SPoC may acquire the data. SPoCs must not acquire the data via a CSP or using automated systems until after the JP has signed the order approving the grant. The one month time limit will commence from the date of the JPs signature giving approval.

The National Anti Fraud Network (NAFN)

5. The National Anti-Fraud Network provides a SPoC service to local authorities, precluding each authority from the requirement to maintain their own trained staff and allowing NAFN to act as a source of expertise. Local authorities using the NAFN SPoC service will still be responsible for submitting any applications to the JP and a designated person in the local authority is still required to scrutinise and approve any applications. The accredited SPoCs at NAFN will examine the applications independently and provide advice to applicants and designated persons to ensure the local authority acts in an informed and lawful manner.
6. The local authority investigator (i.e. the applicant) will then submit the relevant judicial application/order form, the RIPA application (authorisation or notice) and any supporting material to the JP. As above, following a private hearing, the JP will complete the order section of the judicial application/order form, reflecting their decision. The local authority investigator will then upload a copy of this order to the NAFN SPOC.
7. The NAFN SPoC will then acquire the CD on behalf of the local authority in an efficient and effective manner.

Consequential Acquisition

8. Section 3.31 of the Code of Practice for the Acquisition and Disclosure of CD outlines that a designated person may, at the time of granting an authorisation or notice for service usage data, also authorise the consequential acquisition of specific subscriber information. The designated person may only do so to the extent where it is necessary and proportionate. The consequential acquisition may only be for subscriber data, not traffic data, which local authorities may not acquire nor service usage data. Where a SPoC has been authorised to engage in conduct to obtain details of a person to whom a service has been provided and concludes that data is held by a CSP from which it cannot be acquired directly, the SPoC may provide the CSP with details of the authorisation granted by the designated person in order to seek disclosure of the required data¹⁴.
9. In cases where an authorisation or notice seeks to acquire consequential acquisition of specific subscriber information the JP will assess this as part of his/her consideration. The local authority investigator should be prepared to explain to the JP the reasoning behind the request for consequential acquisition and be able to show how it meets the necessity and proportionality tests.
10. In cases where consequential acquisition is approved, but where a notice is required (which must specify the name of the CSP to whom it is given, and be signed by the designated person), a further grant of a notice will be required. This is a new legal instrument and therefore will require further approval to the designated person and the JP, despite authority for the human rights interference having already been given.

¹⁴ Acquisition and Disclosure of Communications Data Code of Practice, Paragraph 3.30.



Home Office

ISBN: 978-1-78246-004-6

Published by the Home Office © Crown Copyright 2012



75% recycled
This publication is printed on 75% recycled paper

Appendix 9

Protection of Freedoms Act 2012 – changes to provisions under the Regulation of Investigatory Powers Act 2000 (RIPA)



Home Office

Home Office guidance for
Magistrates' Courts in England
and Wales for a local authority
application seeking an order
approving the grant or renewal of a
RIPA authorisation or notice

October 2012

Contents

1. Introduction.....	5
2. Local Authority use of RIPA investigatory techniques.....	6
Local Authority Functions.....	6
Use of Investigatory Techniques.....	6
-Directed surveillance.....	7
-Covert Human Intelligence Source (CHIS).....	8
-Communications data.....	9
3. General RIPA principles.....	10
Is a RIPA Authorisation Required?.....	10
Necessity.....	10
Proportionality.....	10
Collateral Intrusion.....	11
4. The Local Authority RIPA process and the role of the JP.....	12
Overview of the Process.....	12
Role of the Justice of the Peace.....	14
Definition of a Local Authority.....	15
Time limits.....	15
Directed Surveillance.....	16
Covert Human Intelligence Sources.....	18
Communications Data.....	20
5. Procedure and decision.....	22
Relevant Magistrates' Court Rules.....	22
Urgent Cases.....	22
Forms.....	22
Local Authority Representation.....	23
Decision.....	23
6. Other sources of reference.....	25
7. Home Office point of contact.....	26
Annex A:	
Procedure flowchart: local authority application to a justice of the peace seeking an order to approve the grant of a RIPA authorisation or notice.....	27
Annex B:	
Judicial Application/Order Form.....	28
Annex C:	
Communications Data RIPA authorisations or notices.....	30
Annex D:	
Regulation of Investigatory Powers (source records) Regulations 2000.....	32

1. INTRODUCTION

1. In the Coalition Agreement the Government gave a commitment to stop local authorities from using covert techniques authorised under the Regulation of Investigatory Powers Act 2000 (“RIPA”) unless they were judicially approved and were required to stop serious crime. Local authorities have been criticised for using surveillance powers in low level cases such as dog fouling and checking that families reside within a school catchment area. The Government has committed to ensuring that local authority use of surveillance should not be allowed in low level cases.
2. This guidance is issued in response to the change in law to introduce independent judicial oversight of local authority use of RIPA. The amendments to RIPA in the Protection of Freedoms Act 2012 that take effect on 1 November 2012¹ will mean that local authority authorisations and notices under RIPA for the use of particular investigatory techniques can only be given effect once an order approving the authorisation or notice has been granted by a Justice of the Peace (“JP”). This process is not part of the local authority investigation but a statutory check on it.
3. The guidance is non-statutory and has been produced to explain the changes that are being made and to provide guidance on the legislative framework, in particular highlighting the tests that the JP must consider. This guidance is intended for Magistrates’ Courts who may be required to consider an application for judicial approval by a local authority. It is supplementary to the legislation and to the statutory Codes of Practice.²
4. Separate guidance is available for Sheriffs in Scotland. Guidance has also been issued to local authorities.

¹ Sections 37 and 38 of the Protection of Freedoms Act 2012 amend RIPA and will come into force on 1 November 2012.

² See page 23 for links to the relevant legislation and codes of practice.

2. LOCAL AUTHORITY USE OF RIPA INVESTIGATORY TECHNIQUES

LOCAL AUTHORITY FUNCTIONS

5. Local authorities have a wide range of functions and are responsible in law for enforcing over 100 separate Acts of Parliament. In particular local authorities investigate offences in the following areas:
 - Trading standards, including action taken against loan sharks and rogue traders, consumer scams, sale of counterfeit goods, unsafe toys and electrical goods.
 - Environmental health, including action against large-scale waste dumping, dangerous workplaces, pest control and the sale of unfit food.
 - Benefit fraud, including action to counter fraudulent claims for housing benefits, investigating 'living together' and 'working whilst in receipt of benefit' allegations and council tax evasion.
6. Local authorities are also responsible for tackling issues as diverse as anti-social behaviour, unlicensed gambling, threats to children in care, underage employment and taxi regulation.

USE OF INVESTIGATORY TECHNIQUES

7. As part of their investigation a local authority may consider that it is appropriate to use a RIPA technique to obtain evidence. In many cases this will be the only way to gather the necessary evidence.
8. The use of an investigative technique can give rise to an interference with an individual's privacy and a public authority will therefore need to consider their obligations under Article 8 of the European Convention on Human Rights (ECHR).
9. RIPA provides a legal framework for a public authority to authorise conduct which engages Article 8 ECHR. It does this by ensuring that use of the relevant techniques are authorised only if the tests of necessity, proportionality and legitimate aim are satisfied. Such a request for authorisation under RIPA is considered by designated senior officers (of a particular rank approved by Parliament) and detailed records must be kept. Independent oversight is provided by the Surveillance Commissioner, the Interception of Communications Commissioner and the Investigatory Powers Tribunal (IPT).³ It is not the function, however, of the Commissioners to keep under review judicial decisions relating to local authority applications.⁴ The IPT will continue to investigate complaints by individuals about the use of RIPA techniques by public bodies, including local authorities. If, following a complaint to them, the IPT does find fault with a RIPA authorisation or notice it has the power to quash the JP's order which approved the grant or renewal of the authorisation or notice.⁵
10. Local authorities use three investigatory techniques that can be authorised under RIPA:
 - Directed surveillance
 - Use of a covert human intelligence source
 - Obtaining and disclosing communications data
11. RIPA does not allow the use of any other covert techniques by local authorities to be authorised. In particular, a local authority cannot be authorised under RIPA to intercept the **content** of a communication.

³ More information on the Investigatory Powers Tribunal can be found at www.ipt-uk.com.

⁴ See section 57 (4A) and section 62(2A) RIPA.

⁵ See section 67(7)(aa) RIPA.

DIRECTED SURVEILLANCE

12. **‘Directed’ surveillance** (DS) is essentially covert surveillance which is not intrusive surveillance.
13. Intrusive surveillance is surveillance carried out in relation to residential premises (including hotel bedrooms, prison cells and rented accommodation), premises where legal consultations take place or private vehicles (including hire or company cars, boats or caravans)⁶. Local authorities cannot authorise intrusive surveillance under RIPA.
14. For the purposes of RIPA, surveillance is “directed” if it is:
 - covert, but not intrusive surveillance (i.e. it takes place somewhere other than residential premises, particular premises where legal consultations take place or private vehicles);
 - conducted for the purposes of a specific investigation or operation e.g. pre-planned against a specific individual or group;
 - likely to result in the obtaining of private information about a person; and
 - conducted otherwise than as an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable to seek an authorisation under RIPA⁷.
15. Surveillance is covert if it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place⁸.
16. Further guidance on the definition of “directed surveillance” is set out in Chapter 2 of the Covert Surveillance and Property Interference Code of Practice⁹.

EXAMPLE

Kent Trading Standards authorised directed surveillance to follow a rogue trader engaged in landscape gardening. The trader was known to ‘cold call’ vulnerable people and charge them over the odds for little work. A previous case involved him cold calling a blind elderly woman, charging her £700 to cut her very small lawn, taking her to the bank in the local town and leaving her there to find her own way home. The surveillance operation resulted in the man’s arrest, the seizure of his van by the police as it was uninsured and the discovery of offensive weapons in the van.

6 Intrusive surveillance is defined in section 26(3) of RIPA. In addition, article 3 of the Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultation) Order 2010 [S.I. 2010/461] provides that surveillance of legal consultations taking place in the premises listed in article 3(2) is also to be treated as intrusive surveillance.

7 See section 26(3) RIPA for the full definition.

8 See section 26(9)(a) RIPA.

9 See page 23 for links to the relevant legislation and codes of practice.

COVERT HUMAN INTELLIGENCE SOURCES

17. **Covert Human Intelligence Sources** (CHIS) include undercover officers, public informants and people who make test purchases.
18. For the purposes of RIPA¹⁰, a person is a CHIS if:
- he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph b) or c);
 - he covertly uses such a relationship to obtain information or to provide access to any information to another person; or
 - he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.
19. A local authority authorisation for the conduct and use of a CHIS may include:
- someone employed or engaged by a local authority to hide their true identity or motivation and covertly use a relationship to obtain information and disclose it to the local authority (an undercover officer); or
 - a member of the public who provides a tip-off to a local authority and is asked to go back and obtain further information by establishing or continuing a relationship whilst hiding their true motivation (an informant).
20. Further guidance on the definition of CHIS is set out in Chapter 2 of the Covert Human Intelligence Sources Code of Practice.¹¹

EXAMPLE

Norfolk County Council received reports questioning whether meat being sold by a butcher on a market stall was fit for human consumption. A joint investigation was run with the District Council Environmental Services. The source of the meat was unknown. A test purchase was carried out. Offences were revealed. The butcher was successfully prosecuted for offences relating to the failure to dispose of animal by products correctly and for food hygiene offences.

¹⁰ See section 26(8) RIPA.

¹¹ See Section 6 for links to the relevant legislation and code of practice.

COMMUNICATIONS DATA

21. Communications data (CD) is the ‘who’, ‘when’ and ‘where’ of a communication, but not the ‘what’ (i.e. the content of what was said or written). CD means any of the following:
 - **‘Traffic Data’** is information about a communication and the equipment used in transmitting it (e.g. information about the location of mobile phones, routing information such as IP address allocation)¹²;
 - **‘Service Use Information’** is information about the use a person makes of a postal or telecommunications service (e.g. itemised telephone call records, records of connection to internet services, timing and duration of service usage)¹³;
 - **‘Subscriber Information’** is information that communications service providers (CSPs) hold about people to whom they provide a service (e.g. names, addresses, telephone numbers)¹⁴.
22. Further guidance on the definition of CD is set out in Chapter 2 of the Acquisition and Disclosure of Communications Data Code of Practice¹⁵.
23. Under RIPA a local authority can only authorise the acquisition of the less intrusive types of CD: service use and subscriber information. Under no circumstances can local authorities be authorised to obtain traffic data under RIPA.
24. Local authorities are not permitted to intercept the content of any person’s communications and it is an offence to do so without lawful authority.

EXAMPLE

Leicestershire County Council Trading Standards Service used CD during an investigation into car clocking. Two individuals purchased high mileage cars via vehicle auction sales and reduced their odometer readings using bespoke mileage correction equipment. Cars were subsequently sold to unsuspecting private buyers together with altered MOT certificates and falsified service histories. The criminal offences under investigation were: conspiracy to undertake a business for a fraudulent purpose, supplying goods with a false trade description and engaging in unfair commercial practice. This form of acquisitive crime allows the fraudster to make substantial financial gains whilst the purchaser is left with a vehicle of minimal resale value. This activity also harms the collective interest of businesses that operate within the retail car trade. An array of names, addresses and telephone numbers were provided by the defendants in advertisements, auction records and sales invoices. Subscriber checks acquired in relation to the telephone numbers enabled investigators to link both defendants to the purchase and sale of around forty vehicles.

12 See section 21(4)(a) and 21(6) RIPA for the full definition, and paragraphs 2.19 to 2.22 of the Acquisition and Disclosure of CD Code of Practice for further guidance and examples of traffic data.

13 See section 21(4)(b) RIPA for the full definition and paragraphs 2.23 to 2.24 of the Acquisition and Disclosure of CD Code of Practice for further guidance and examples of service use information.

14 See section 21(4)(c) RIPA for the full definition and paragraphs 2.25 to 2.29 of the Acquisition and Disclosure of CD Code of Practice for further guidance and examples of subscriber information.

15 See Section 6 for links to the relevant legislation and codes of practice.

3. GENERAL RIPA PRINCIPLES

IS A RIPA AUTHORISATION REQUIRED?

25. A local authority using investigative techniques will need to consider whether or not the use of that technique engages Article 8 of the ECHR. If it does, then obtaining an authorisation under RIPA is one way for the local authority to ensure that their activity is conducted lawfully and compatibly with the ECHR.
26. If the local authority is proposing to act covertly but Article 8 is not engaged then no RIPA authorisation is necessary. For instance, a local authority may covertly monitor traffic flows or check the volume of people using a particular facility without obtaining private information about anyone. The local authority will assess whether they should obtain authorisation under RIPA.

NECESSITY

27. A RIPA authorisation may only be granted if the authorising officer believes that the conduct is necessary for one or more of the statutory purposes. The statutory purposes in RIPA mirror the legitimate aims in Article 8(2) ECHR. The RIPA Orders¹⁶ provide that local authorities may only authorise the use of covert techniques for the purpose of ‘the prevention or detection of crime or the prevention of disorder’¹⁷.
28. Preventing and detecting crime goes beyond the prosecution of offenders and includes actions taken to avert, end or disrupt the commission of criminal offences. The local authority must be satisfied that there is an identifiable offence to detect or prevent before authorising the use of any covert technique under RIPA.

PROPORTIONALITY

29. The authorising officer must also believe that the authorised conduct is proportionate to what is sought to be achieved. This involves balancing the seriousness of the intrusion into the privacy of the subject of the investigation (or any other person who may be affected) against the need for the activity in investigative terms. If overt investigative methods would be effective, it is unlikely to be proportionate to authorise intrusive covert activity.

¹⁶ For further information refer to: The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (SI 2010 No. 521) and The Regulation of Investigatory Powers (Communications Data) Order 2010 (SI2010 No.480).

¹⁷ There is a further restriction on use of directed surveillance – see paragraph 55 below.

30. The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render intrusive actions proportionate. Similarly, an offence may be so minor that any development of covert techniques would be disproportionate. The following elements of proportionality should therefore be considered:
- Balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
 - Explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
 - Considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
 - Recording, as far as reasonably practicable, what other methods had been considered and why they were not implemented.
31. Particular consideration should be given to circumstances where it is likely that confidential information or matters subject to legal privilege may be acquired. This includes but is not limited to communications between a professional legal adviser and his client, a Member of Parliament and another person on constituency matters, confidential personal information, or confidential journalistic information¹⁸.

COLLATERAL INTRUSION

32. The risk and proportionality of interfering with the privacy of people not connected with the investigation must also be weighed and, where possible, steps taken to mitigate it.

¹⁸ See Covert Surveillance and Property Interference: Code of Practice, chapter 4 and Covert Human Intelligence Sources: Code of Practice, chapter 4.

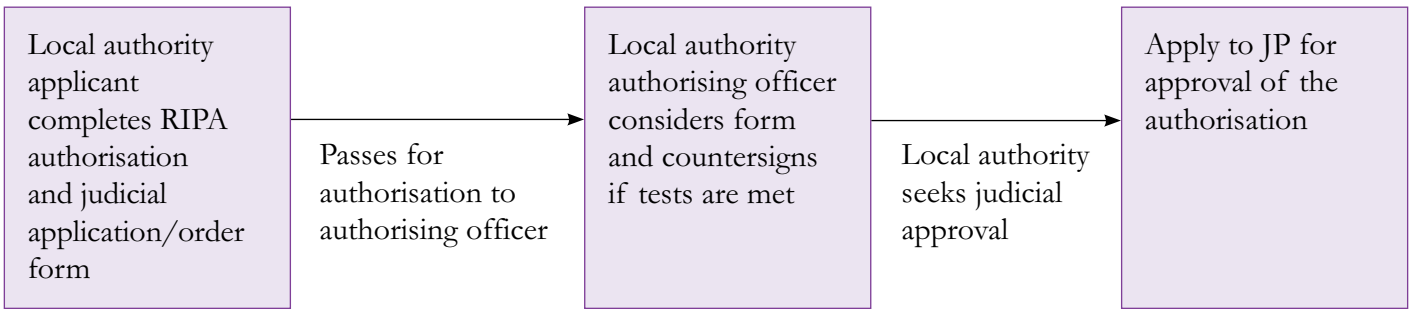
4. THE LOCAL AUTHORITY RIPA PROCESS AND THE ROLE OF THE JP

OVERVIEW OF THE PROCESS

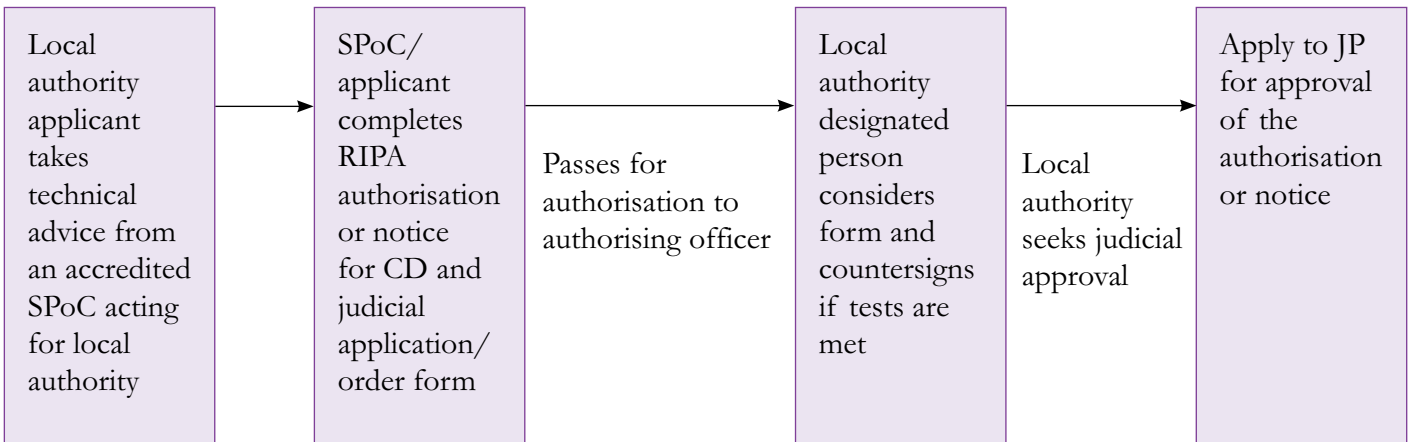
33. The judicial approval process introduced by the Protection of Freedoms Act 2012 and coming into effect on 1 November 2012 applies to situations where a local authority applicant (i.e. the investigating officer - the person involved in conducting an investigation or operation) is intending to use a covert investigatory technique and the local authority takes the view that use of that technique should be authorised under RIPA.
34. Current practice is that the local authority will authorise internally. The applicant will complete a written RIPA authorisation or notice form setting out for consideration by the authorising officer or, for CD, the designated person; why use of a particular technique is necessary and proportionate in their investigation. This authorising officer or designated person holds a prescribed office in the relevant local authority and will consider the application, recording his/her considerations and countersign the form if he/she believes the statutory tests are met.
35. In the case of CD the RIPA authorisation or notice will have also been scrutinised by a single point of contact (a 'SPoC'). The SPoC is either an accredited individual or a group of accredited individuals trained to facilitate lawful acquisition of communications data and effective co-operation between a public authority and Communication Service Providers (CSPs). An accredited SPoC promotes efficiency and good practice in ensuring only practical and lawful requests for CD are made¹⁹. For many local authorities the SPoC services are carried out by the National Anti-Fraud Network ('NAFN') (More details on the SPoC role, NAFN and consequential acquisition of CD is contained at Annex C).
36. These practices will continue. However, there will now be an additional stage in the process for all three techniques. After the form has been countersigned the local authority will seek judicial approval for their RIPA authorisation or notice. The JP will decide whether a local authority grant or renewal of an authorisation or notice to use RIPA should be approved and it will not come into effect unless and until it is approved by a JP. Although it is possible for local authorities to request judicial approval for the use of more than one technique at the same time, in practice, as different considerations need to be applied to different techniques, this would be difficult to perform with the degree of clarity required. As a rule local authorities should aim to submit separate authorisations or notices to authorise the use of different RIPA techniques.

37. The process is outlined below:

DIRECTED SURVEILLANCE / CHIS (COVERT HUMAN INTELLIGENCE SOURCE)



COMMUNICATIONS DATA



THE ROLE OF THE JUSTICE OF THE PEACE

38. The role of the JP is set out in section 23A RIPA (for CD) and section 32A RIPA (for directed surveillance and CHIS).
39. These sections provide that the authorisation, or in the case of CD, the notice, shall not take effect until the JP has made an order approving such an authorisation or notice. The matters on which the JP needs to be satisfied before giving judicial approval are that:
- there were reasonable grounds for the local authority to believe that the authorisation or notice was necessary and proportionate and there remain reasonable grounds for believing that these requirements are satisfied at the time when the JP is considering the matter²⁰;
 - in the case of a CHIS authorisation, that there were reasonable grounds for the local authority to believe that arrangements exist for the safety and welfare of the source that satisfy section 29(5) RIPA and there remain reasonable grounds for believing that these requirements are satisfied at the time when the JP is considering the matter²¹;
 - in the case of a CHIS authorisation, that there were reasonable grounds for the local authority to believe that the requirements imposed by Regulation of Investigatory Powers (Juvéniles) Order 2000²² were satisfied and there remain reasonable grounds for believing that these requirements are satisfied at the time when the JP is considering the matter²³;
 - the local authority application has been authorised by a designated person / authorising officer.²⁴;
 - the grant of the authorisation or in the case of CD, the notice, was not in breach of any restriction imposed by virtue of an order made under the following sections of RIPA:
 - 25(3) (for communications data),
 - 29(7)(a) (for CHIS),
 - 30(3) (for directed surveillance and CHIS)²⁵:
 - any other conditions that may be provided for by an order made by the Secretary of State were satisfied.
40. A detailed explanation of what is required for each of these techniques is set out in paragraphs 48 – 83 below.
41. The same considerations apply where a local authority is seeking judicial approval to continue using a technique (i.e. a renewal). Although the JP will wish to examine whether the case for a more sustained interference of Article 8 still meets the principle of proportionality. In particular he or she will want to consider the content and value of the information obtained so far.²⁶

20 For CD see sections 23A(3) and (4) RIPA. For directed surveillance see section 32A(3) RIPA. For CHIS see section 32A(5) RIPA insofar as it relates to the requirements imposed by section 29(2)(a) and (b) RIPA.

21 See section 32A(5) RIPA insofar as it relates to the requirements imposed by section 29(2)(c) RIPA.

22 SI 2000/2793.

23 See section 32A(5) RIPA insofar as it relates to requirements imposed by virtue of section 29(7)(b) RIPA.

24 For communications data, see section 23A(5)(a)(i) RIPA. For directed surveillance, see section 32A(4)(a)(i) RIPA. For CHIS, see section 32A(6)(a)(i) RIPA. For more detailed guidance on the ranks of designated individuals see paragraphs 51-54, 67-71 and 79-82 of this guidance.

25 For communications data, see section 23A(5)(a)(ii) RIPA. For directed surveillance, see section 32A(4)(a)(ii) RIPA. For CHIS, see section 32A(6)(a)(ii) RIPA. For more detailed guidance on the restrictions imposed under the provisions referred to see paragraphs 55, 65, 66, 72, 73, and 83 below.

26 See the Covert Surveillance and Property Interference Code of Practice, Chapter 5, paragraphs 5.12-5.16, Covert Human Intelligence Sources Code of Practice, Chapter 5, paragraphs 5.17-5.22 and Acquisition and Disclosure of Communications Data Code of Practice, Chapter 3, paragraphs 3.46-3.48

DEFINITION OF A LOCAL AUTHORITY

42. RIPA defines a local authority as:

- the Common Council of the City of London in its capacity as a local authority;
- a London borough council;
- a county council or district council in England;
- a county council or county borough council in Wales; and
- the Council of the Isles of Scilly.

43. The definition of local authorities as set out in the relevant statutory instruments (Nos.480 and 521 of 2010) includes metropolitan borough councils by virtue of the Local Government Acts. There is no category of 'unitary' or 'metropolitan' or 'city' or 'borough' councils that does not fall within the definition of 'district' or 'county' council as set out in those Acts.

44. This statutory definition of a local authority does not include local authority umbrella organisations or consortia. However, a local authority can use an external contactor to carry out directed surveillance or to establish or maintain a relationship for a covert purpose. In these circumstances then that body or person must be clearly identified in the application to the JP.

TIME LIMITS

45. The current time limits for an authorisation or notice will remain.²⁷ That is: three months for directed surveillance and twelve months for a CHIS (one month if the CHIS is under 18). Authorisations and notices for CD will be valid for a maximum of one month from the date the JP has approved the grant. This means that the conduct authorised should have been commenced or the notice served within that month.

46. A renewal must be authorised prior to the expiry of the original authorisation, but it runs from the expiry date and time of that original authorisation. Authorisations may be renewed more than once if still considered necessary and proportionate.

47. Applications for renewals should not be made until shortly before the original authorisation period is due to expire. It is impossible to give a definitive period prior to expiry when an application for renewal should be made, but local authorities must take account of factors which may delay the renewal process (e.g. intervening weekends or the availability of the authorising officer and a JP to grant approval).

²⁷ See section 43 RIPA

DIRECTED SURVEILLANCE

Authorisation Requiring Judicial Approval

48. Under section 28(1) RIPA, local authorities may authorise the use of directed surveillance. A local authority will need to seek judicial approval of the grant or renewal of any authorisation under RIPA.

Necessity and Proportionality

49. The requirements of necessity and proportionality are fundamental parts of the RIPA authorisation. Further guidance on these can be found in section 3 of this guidance and the relevant Code of Practice.
50. A local authority can only be authorised under RIPA to carry out directed surveillance where it:
- **is necessary for the purpose of preventing or detecting crime or of preventing disorder**²⁸; and
 - Meets the ‘crime threshold’ set out in secondary legislation which comes into effect on 1 November 2012. This is explained further in paragraph 55 of this guidance.

Authorising Officer

51. For the purposes of directed surveillance the authorising officer in a local authority is the **Director, Head of Service, Service Manager or equivalent**²⁹.
52. An individual holding a more senior rank may also be a authorising officer³⁰.
53. Where it is likely that knowledge of confidential information or matters subject to legal privilege will be acquired, the directed surveillance may only be authorised by the **Head of Paid Service**, or (in his/her absence) the person acting as the Head of Paid Service³¹. Local authorities are also subject to additional restrictions in relation to legal professional privilege, which are described further below.
54. If there is any doubt regarding sufficiency of rank the JP should request the local authority representative obtain confirmation from their Local Authority Monitoring Officer who will be able to advise them.

28 See section 28(2) and (3) RIPA which set out the necessity grounds in general. See also article 5 and the entry for local authorities (i.e. any county council, etc) in the Schedule to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (SI 2010/521) which limits local authorities to the necessity ground in section 28(3)(b) RIPA. Local authorities cannot authorise directed surveillance for the purpose of preventing disorder unless this involves a criminal offence which meets the threshold set out at paragraph 55.

29 See article 3(2) and the entry for local authorities (i.e. any county council, etc) in the Schedule to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (SI 2010/521).

30 See article 3(3) of the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (SI 2010/521).

31 See the Covert Surveillance and Property Interference Code of Practice, Chapter 4 (particularly paragraphs 4.3 and 4.14) and Annex A.

Additional Restrictions and Conditions

Crime Threshold

55. Under the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010³² local authorities may only authorise use of directed surveillance where they are investigating crime and where the criminal offence being investigated meets one of the following conditions:
- (a) the offence is punishable, whether on summary conviction or on indictment, by a maximum term of at least 6 months of imprisonment, or
 - (b) the offence is an offence under:
 - (i) sections 146, 147 or 147A of the Licensing Act 2003 or
 - (ii) section 7 of the Children and Young Persons Act 1933.

Intrusive Surveillance

56. Local authorities cannot authorise the use of intrusive surveillance under RIPA.
57. Intrusive surveillance is surveillance that is carried out in relation to anything taking place on any residential premises or in any private vehicle³³. Images taken with equipment which consistently provide the same detail or quality as if they were taken in residential premises or private vehicles constitutes ‘intrusive’ surveillance.
58. Additionally, surveillance of any of the following premises whilst they are being used for legal consultation is to be treated as intrusive surveillance:
- (a) any place in which persons who are serving sentences of imprisonment or detention, remanded in custody or committed in custody for trial or sentence may be detained;
 - (b) any place in which persons may be detained under relevant immigration legislation;
 - (c) any place in which persons may be detained under the Mental Health Act 1983;
 - (d) police stations;
 - (e) any place of business of any professional legal adviser;
 - (f) any place used for the sittings and business of any court, tribunal, inquest or inquiry³⁴.

³² S.I. 2010/521, see article 7A. This restriction comes into force on 1 November 2012.

³³ See section 26(3) RIPA for full definition.

³⁴ For the definition of ‘legal consultation’ and the full definitions of the relevant premises, see articles 2 and 3 of the Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultation) Order 2010 (S.I. 2010/461).

COVERT HUMAN INTELLIGENCE SOURCES

Authorisation Requiring Judicial Approval

59. Under section 29(1) RIPA, local authorities may authorise the conduct or use of a CHIS. A local authority will need to seek judicial approval of the grant or renewal of any authorisation under RIPA.
60. The local authority is not required to provide the true identity of the source either on the application form or verbally to the JP.

Necessity and Proportionality

61. The requirements of necessity and proportionality are fundamental parts of the RIPA authorisation. Further guidance on these can be found in section 3 of this guidance and the relevant Code of Practice.
62. A local authority can only be authorised under RIPA for the conduct or use of a CHIS where it is **necessary for the purpose of preventing or detecting crime or of preventing disorder**.³⁵

Arrangements for the safety and security of the CHIS

63. A local authority must have arrangements in place that ensure:
 - an individual in the local authority has day-to-day responsibility for dealing with the source and for the CHIS's security and welfare;
 - an individual in the local authority has general oversight of the use made of the CHIS and for maintaining a record of such use;
 - records relating to the CHIS contain particulars of the matters specified in the Regulation of Investigatory Powers (Source Records) Regulations 2000³⁶;
 - records that disclose the identity of the CHIS will only be available to those who need access to them³⁷.
64. Where a CHIS is under the age of 16 arrangements must also include ensuring that an appropriate adult (usually a parent or carer) is present at every meeting with the local authority³⁸.

Restrictions on use of juveniles

65. A local authority cannot authorise the use of a CHIS under the age of 16 to gather evidence against his parents or carers³⁹.

35 See section 29(2) and (3) RIPA which set out the necessity grounds in general. See also article 5 and the entry for local authorities (i.e. any county council, etc) in the Schedule to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (SI 2010/521) which limits local authorities to the necessity ground in section 29(3)(b) RIPA.

36 SI 2000/2725 attached at Annex D.

37 See section 29(5) RIPA.

38 See article 4, Regulation of Investigatory Powers (Juveniles) Order 2000 (SI 2000/2793).

39 See article 3, Regulation of Investigatory Powers (Juveniles) Order 2000 (SI 2000/2793).

66. A local authority cannot authorise the use of a CHIS under the age of 18 without carrying out a special risk assessment in relation to any risk of physical injury or psychological distress to the source that may arise. The authorising officer must also be satisfied that any risks identified are justified and have been explained to and are understood by the CHIS. If the local authority is authorising the use of a CHIS against his parents or carers particular consideration must be given to whether this is justified⁴⁰.

Authorising Officer

67. Except as set out below, for the purposes of CHIS the authorising officer is the **Director, Head of Service, Service Manager or equivalent**⁴¹.
68. An individual holding a more senior rank may also be a authorising officer⁴².
69. Where it is likely that knowledge of confidential information or matters subject to legal privilege will be acquired, the authorising officer is the **Head of Paid Service**, or (in his/her absence) the person acting as the Head of Paid Service⁴³. Local authorities are also subject to additional restrictions in relation to legal professional privilege, which are described further below.
70. Where the CHIS is a juvenile or a vulnerable individual the authorising officer is the **Head of Paid Service** or (in his/her absence) the person acting as the Head of Paid Service⁴⁴.
71. If there is any doubt regarding sufficiency of rank the JP should request the local authority representative obtain confirmation from their Local Authority Monitoring Officer who will be able to advise them.

Additional Restrictions and Conditions

Vulnerable Individuals

72. A vulnerable individual is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself or unable to protect himself against significant harm or exploitation. A vulnerable individual should only be authorised to act as a CHIS in the most exceptional circumstances⁴⁵.

Matters subject to Legal Privilege

73. Where the activities of a CHIS will result in the CHIS obtaining, providing access to or disclosing matters subject to legal privilege, a local authority must obtain prior approval from the Surveillance Commissioners before authorising such conduct⁴⁶. The local authority should provide the JP with copies of any such approval as part of their application process.

40 See article 5, Regulation of Investigatory Powers (Juveniles) Order 2000 (SI 2000/2793).

41 See article 3(2) and the entry for local authorities (i.e. any county council, etc) in the Schedule to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (SI 2010/521).

42 See article 3(3) of the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (SI 2010/521).

43 See Annex A of both the Covert Human Intelligence Sources Code of Practice and the Covert Surveillance and Property Interference Code of Practice.

44 See paragraphs 4.22 and 4.23 of the Covert Human Intelligence Sources Code of Practice.

45 See paragraph 4.22 of the Covert Human Intelligence Sources Code of Practice.

46 See Parts 2 and 3 of the Regulation of Investigatory Powers (Covert Human Intelligence Sources: Matters Subject to Legal Privilege) Order 2010 (SI 2010/123)

COMMUNICATIONS DATA

Authorisation Requiring Judicial Approval

74. A local authority will need to seek judicial approval of the grant or renewal of an “authorisation” or of the giving or renewal of a “notice” under RIPA.
75. Under section 22(3) RIPA, local authorities may authorise the acquisition of CD by an ‘authorisation’. An authorisation will be used where the designated person is authorising a person working in the same public authority to engage in specific conduct. This will normally be the public authority’s SPoC. Under section 22(4) RIPA, local authorities may serve a ‘notice’ on a CSP to obtain and disclose the data themselves⁴⁷.
76. The authorisation or notice under RIPA may only relate to Service Use Information or Subscriber Information (see paragraph 21-24 of this guidance). CD requests may seek to acquire consequential acquisition of specific subscriber information. The necessity and proportionality of acquiring consequential acquisition will be assessed by the JP as part of his consideration (see Annex C for considerations relating to CD authorisations and notices).

Necessity and Proportionality

77. The requirements of necessity and proportionality are fundamental parts of the RIPA authorisation. Further guidance on these can be found in section 3 of this guidance and the relevant Codes of Practice.
78. A local authority can only be authorised under RIPA to obtain CD where it is necessary **is necessary for the purpose of preventing or detecting crime or of preventing disorder**⁴⁸.

Authorising officer / Designated Person

79. For the purposes of CD the authorising officer / designated person is the **Director, Head of Service, Service Manager or equivalent**⁴⁹.
80. An individual holding a more senior rank may also be an authorising officer / designated person⁵⁰.
81. The authorising officer’s counter signature will in all cases show the rank or title of the grade and cover a clear description in his or her own words of what is being authorised and against which subjects or location (‘who, what, where, when and how’). For many CD requests the forms are completed electronically, including the insertion of an electronic signature for the designated person.

47 For further guidance see paragraphs 3. 23 to 3.41 of the Acquisition and Disclosure of Communications Data Code of Practice.

48 See section 22(1) and (2) RIPA which set out the necessity grounds in general. See also article 3(3) and the entry for local authorities (i.e. the Common Council of the City of London, etc) in Schedule 2, Part 2 of the Regulation of Investigatory Powers (Communication Data) Order 2010 (SI 2010/480) which limits local authorities to the necessity ground in section 22(2)(b) RIPA.

49 See article 4(1) and the entry for local authorities (i.e. the Common Council of the City of London, etc) in Schedule 2, Part 2 of the Regulation of Investigatory Powers (Communication Data) Order 2010 (SI 2010/480).

50 See article 4(2) of the Regulation of Investigatory Powers (Communication Data) Order 2010 (SI 2010/480).

82. If there is any doubt regarding sufficiency of rank the JP should request the local authority representative obtain confirmation from their Local Authority Monitoring Officer who will be able to advise them.

Additional Restrictions and Conditions

83. Local authorities may only acquire service use information or subscriber information. They may not acquire traffic data⁵¹.

⁵¹ See article 6(4) and the entry for local authorities (i.e. the Common Council of the City of London, etc) in Schedule 2, Part 2 of the Regulation of Investigatory Powers (Communication Data) Order 2010 (SI 2010/400)

5. PROCEDURE AND DECISION

84. A flowchart at Annex A details each stage of this process from receipt of the local authority application to the decision made by the JP.

RELEVANT MAGISTRATES' COURTS RULES

85. The procedures and practice governing the JP's role in examining and deciding on local authority applications for the use of the techniques regulated by RIPA are covered in England and Wales by court rules.⁵² The Rules set out that the hearing will not be in open court, and no press, public, the subject of the investigation or the subject's legal representative will be present. In order to maintain privacy, notice of the application is not required to the person whom the authorisation or notice concerns or that person's legal representatives.
86. The form and supporting papers must by themselves make the case. It is not sufficient for the local authority to provide oral evidence where this is not reflected or supported by the form and papers. However, the JP may wish to note on the form any additional information he or she has received during the course of the hearing rather than requiring the application to be re-submitted. Information fundamental to the case must not be submitted in this manner.

URGENT CASES

87. No RIPA authority is required in immediate response to events or situations where it is not reasonably practicable to obtain it (for instance when criminal activity is observed during routine duties and officers conceal themselves to observe what is happening).
88. On the rare occasions where out of hours access to a JP is required then it will be for the local authority to make local arrangements with the relevant HM Courts and Tribunals Service (HMCTS) legal staff. In these cases the local authority will need to provide two partially completed judicial application/order forms so that one can be retained by the JP. The local authority will provide a copy of the signed application/order form to the court the next working day in the same way as applications for other urgent matters.

FORMS

89. The local authority will provide the JP with a copy of the original RIPA authorisation or notice and the supporting documents setting out the case.⁵³ This forms the basis of the authorisation and should contain all information that is relied upon.
90. Local authorities may use the RIPA forms available on the Home Office website⁵⁴. These simply summarise the information that RIPA requires in order to generate a properly considered authorisation for each technique.

⁵² See Part 6 of the Criminal Procedure Rules.

⁵³ No fee is payable for these applications as they are criminal proceedings.

⁵⁴ www.homeoffice.gov.uk/counter-terrorism/regulation-investigation-techniques/ripa-forms

91. There is no requirement in law to use the Home Office forms, but applications must contain all the relevant information. Some local authorities adapt the Home Office forms, for example to incorporate logos or to reflect local procedures or processes.
92. The original RIPA form should be shown to the JP but will be retained by the local authority so that it is available for inspection by the Commissioners' offices and in the event of any legal challenge or investigations by the Investigatory Powers Tribunal. The court must take a copy of the RIPA authorisation / notice. JPs must ensure they have copies of all documentation for storage by HMCTS in compliance with Rule 5 of the Criminal Procedure Rules, and in order to deal with queries and complaints.
93. In addition, the local authority will provide the JP with a partially completed judicial application/order form (at Annex B). The local authority should complete their section of the form before the hearing.
94. This form will be the official record of the JP's decision. However, although the local authority is required to provide a brief summary of the circumstances of the case on the judicial application form, this is supplementary to and does not replace the need to supply the original RIPA authorisation or notice as well.

LOCAL AUTHORITY REPRESENTATION

95. Local authorities will choose the most appropriate representatives to present their RIPA application to the JP. It is expected that most authorities will designate investigative officers under section 223 of the Local Government Act 1972 to appear on their behalf, rather than a solicitor. This is because the local authority investigator knows the most about the investigation and will have determined that use of a covert technique is required in order to progress a particular case. The investigator will make the case on the RIPA authorisation or notice so that the authorising officer or designated person can consider the tests of necessity and proportionality. This does not, however, remove or reduce in any way the duty on the authorising officer to determine whether the tests are met.
96. For CD applications, the local authority may consider it appropriate for the SPoC (single point of contact for CD RIPA authorisations) to attend (see Annex C). Designation under section 223 of the Local Government Act 1972 by way of the local authority Standing Orders will enable investigation staff or SPoCs to attend for this purpose. It is not envisaged that the skills of legally trained personnel will be required to make the case and this would be likely to, unnecessarily, increase the costs of local authority applications.

DECISION

97. The JP should record his/her decision on the order section of the judicial application/order form. The JP will sign, date and endorse the time of decision. A copy will be provided to the local authority.

98. The JP may decide to⁵⁵ –

- **Approve the grant or renewal of an authorisation or notice**

The grant or renewal of the RIPA authorisation or notice will then take effect and the local authority may proceed to use the technique in that particular case.

In relation to CD, the local authority will be responsible for providing a copy of the order to the SPoC .

- **Refuse to approve the grant or renewal of an authorisation or notice**

The RIPA authorisation or notice will not take effect and the local authority may not use the covert technique.

Where an application has been refused the local authority may wish to consider the reasons for that refusal. For example, a technical error in the form may be remedied without the local authority going through the internal authorisation process again. The local authority may then wish to reapply for judicial approval once those steps have been taken.

- **Refuse to approve the grant or renewal and quash the authorisation or notice**

This applies where a magistrates' court refuses to approve the grant, giving or renewal of an authorisation or notice and decides to quash the original authorisation or notice.

The court must not exercise its power to quash that authorisation or notice unless the applicant has had at least 2 business days from the date of the refusal in which to make representations.⁵⁶

⁵⁵ See sections 23B(3) and 32B(3) RIPA.

⁵⁶ See the amended Rule 6 of the Criminal Procedure Rules.

6. OTHER SOURCES OF REFERENCE

- The Regulation of Investigatory Powers Act 2000
<http://www.legislation.gov.uk/ukpga/2000/23/contents>

- RIPA Explanatory Notes
<http://www.legislation.gov.uk/ukpga/2000/23/notes/contents>

- RIPA statutory codes of practice

Covert Surveillance and Property Interference

<http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa/forms/code-of-practice-covert>

Covert Human Intelligence Sources

<http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa/forms/code-of-practice-human-intel>

Acquisition & Disclosure of Communications Data

<http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa/forms/code-of-practice-acquisition>

- SI 2000 No.2793 (The Regulation of Investigatory Powers (Juveniles) Order 2000
<http://www.legislation.gov.uk/uksi/2000/2793/made>
- SI 2010 No.480 - Regulation of Investigatory Powers (Communications Data) Order 2010
<http://www.legislation.gov.uk/uksi/2010/480/contents>
- SI 2010 N0.521 - Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010
<http://www.legislation.gov.uk/uksi/2010/9780111490365/contents>
- SI 2010 No.461 (The Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010
<http://www.legislation.gov.uk/uksi/2010/461/contents>
- SI 2012 No.1500 (The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012)
<http://www.legislation.gov.uk/uksi/1500/contents>

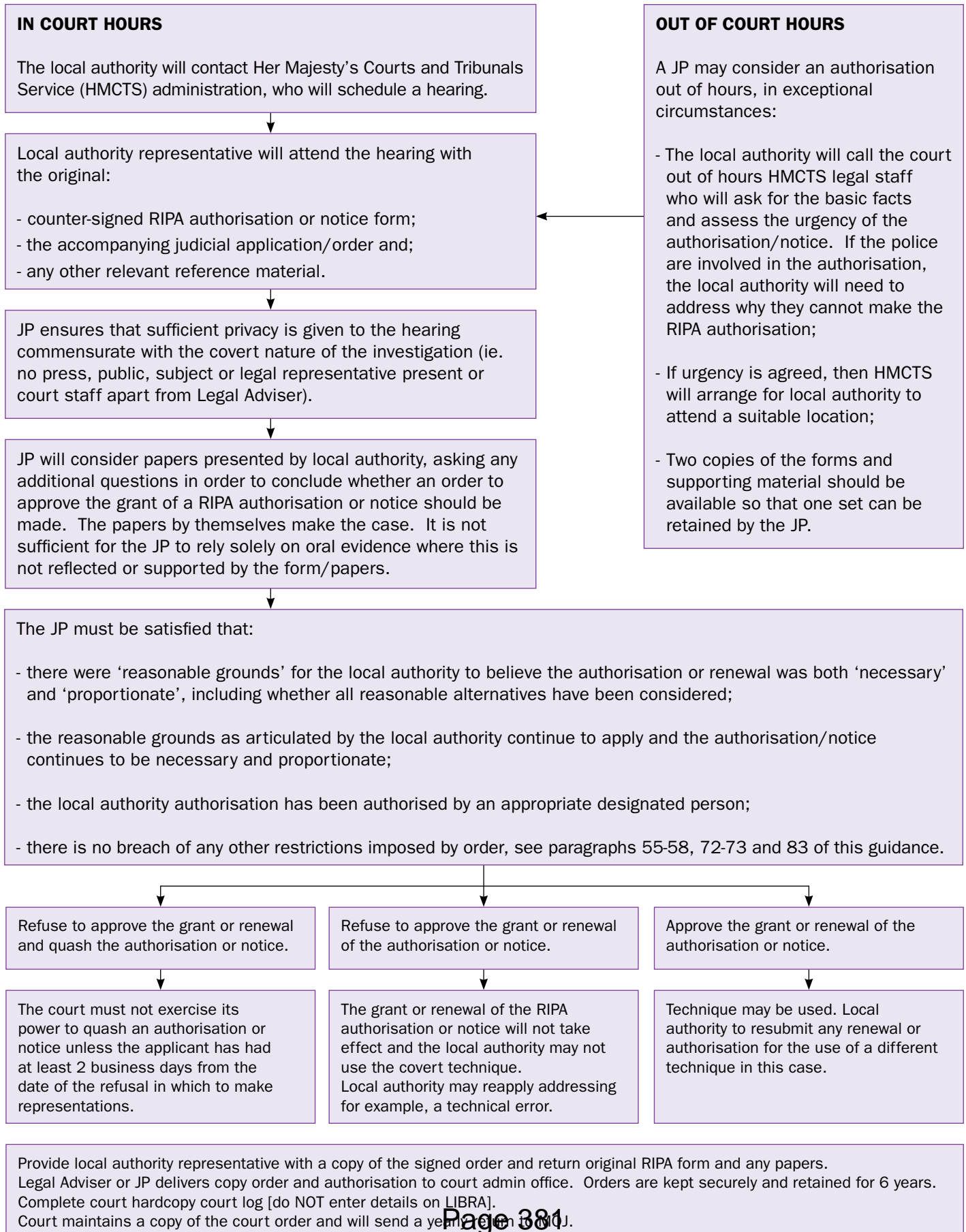
7. HOME OFFICE POINT OF CONTACT

Further information is available on request from:

RIPA Team
Home Office
5th Floor Peel Building
2 Marsham Street
London SW1P 4DF
Email: commsdata@homeoffice.x.gsi.gov.uk

ANNEX A

PROCEDURE: LOCAL AUTHORITY APPLICATION TO A JUSTICE OF THE PEACE SEEKING AN ORDER TO APPROVE THE GRANT OF A RIPA AUTHORISATION OR NOTICE



ANNEX B

Application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Local authority:.....

Local authority department:

Offence under investigation:.....

Address of premises or identity of subject:

.....

.....

Covert technique requested: (tick one and specify details)

Communications Data

Covert Human Intelligence Source

Directed Surveillance

Summary of details

.....

.....

.....

.....

.....

.....

Note: this application should be read in conjunction with the attached RIPA authorisation/RIPA application or notice.

Investigating Officer:.....

Authorising Officer/Designated Person:

Officer(s) appearing before JP:

Address of applicant department:.....

.....

Contact telephone number:.....

Contact email address (optional):

Local authority reference:

Number of pages:.....

Order made on an application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Magistrates' court:.....

Having considered the application, I (tick one):

- am satisfied that there are reasonable grounds for believing that the requirements of the Act were satisfied and remain satisfied, and that the relevant conditions are satisfied and I therefore approve the grant or renewal of the authorisation/notice.
- refuse to approve the grant or renewal of the authorisation/notice.
- refuse to approve the grant or renewal and quash the authorisation/notice.

Notes

.....
.....
.....
.....
.....

Reasons

.....
.....
.....
.....
.....
.....

Signed:

Date:

Time:

Full name:

Address of magistrates' court:

COMMUNICATIONS DATA RIPA AUTHORISATIONS OR NOTICES

Single Point of Contact (SPoC)

1. For CD requests, a Single Point of Contact (SPoC) undertakes the practical facilitation with the communications service provider (CSP) in order to obtain the CD requested. They will have received training specifically to facilitate lawful acquisition of CD and effective co-operation between the local authority and communications service providers.
2. Local authorities unable to call upon the services of an accredited SPoC should not undertake the acquisition of CD.
3. For CD requests the Home Office envisages that the local authority may also choose to authorise, under Section 223 of the Local Government Act, their SPoC in order that they may appear in front of the JP if required. In cases where the type of CD or its retrieval is technically complex and the JP wants to satisfy him/herself that the CD sought meets the test, then the SPoC may be best placed to explain the technical aspects.

The National Anti Fraud Network (NAFN)

4. The National Anti-Fraud Network provides a SPoC service to local authorities, preventing each authority from the requirement to maintain their own trained staff and allowing NAFN to act as a source of expertise. Local authorities using the NAFN SPoC service will still be responsible for submitting any applications and a designated person in the local authority is still required to scrutinise and approve any applications. The accredited SPoCs at NAFN will examine the applications independently and provide advice to applicants and designated persons to ensure the local authority acts in an informed and lawful manner.
5. The local authority investigator (i.e. the applicant) will then submit the relevant judicial application/order form, the RIPA authorisation or notice and any supporting material to the JP. As above, following a private hearing, the JP will complete an order reflecting their decision. The local authority investigator will then upload a copy of this order to the NAFN SPoC.
6. The NAFN SPoC will then acquire the CD on behalf of the local authority in an efficient and effective manner.

Consequential Acquisition

7. Section 3.31 of the Code of Practice for the Acquisition and Disclosure of CD outlines that a designated person may, at the time of granting an authorisation or notice for service usage data, also authorise the consequential acquisition of specific subscriber information. The designated person may only do so to the extent where it is necessary and proportionate. The consequential acquisition may only be for subscriber data, not traffic data, which local authorities may not acquire nor service usage data. Where a SPoC has been authorised to engage in conduct to obtain details of a person to whom a service has been provided and concludes that data is held by a CSP from which it cannot be acquired directly, the SPoC may provide the CSP with details of the authorisation granted by the designated person in order to seek disclosure of the required data⁵⁷.
8. In cases where an authorisation or notice seeks to acquire consequential acquisition of specific subscriber information the JP will assess this as part of his/her consideration. The local authority investigator should be prepared to explain to the JP the reasoning behind the request for consequential acquisition and be able to show how it meets the necessity and proportionality tests.
9. In cases where consequential acquisition is approved, but where a notice is required (which must specify the name of the CSP to whom it is given, and be signed by the designated person), a further grant of a notice will be required. This is a new legal instrument and therefore will require a further visit to the designated person and the JP, despite authority for the human rights interference having already been given.

ANNEX D

REGULATION OF INVESTIGATORY POWERS (SOURCE RECORDS) REGULATIONS 2000

The following matters are specified for the purposes of paragraph (d) of section 29(5) of the 2000 Act (as being matters particulars of which must be included in the records relating to each source):

- (a) the identity of the source;
- (b) the identity, where known, used by the source;
- (c) any relevant investigating authority other than the authority maintaining the records;
- (d) the means by which the source is referred to within each relevant investigating authority;
- (e) any other significant information connected with the security and welfare of the source;
- (f) any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (d) has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source;
- (g) the date when, and the circumstances in which, the source was recruited;
- (h) the identities of the persons who, in relation to the source, are discharging or have discharged the functions mentioned in section 29(5)(a) to (c) of the 2000 Act or in any order made by the Secretary of State under section 29(2)(c);
- (i) the periods during which those persons have discharged those responsibilities;
- (j) the tasks given to the source and the demands made of him in relation to his activities as a source;
- (k) all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;
- (l) the information obtained by each relevant investigating authority by the conduct or use of the source;
- (m) any dissemination by that authority of information obtained in that way; and
- (n) in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority.



Home Office

ISBN: 978-1-78246-005-3

Published by the Home Office © Crown Copyright 2012



75% recycled
This publication is printed on 75% recycled paper

Appendix 10

Surveillance Quality Monitoring Form

Application Ref No:	
Type of application:	RIPA / CHIS / Non-RIPA
Checked by:	Name: Title:
Date:	

1. Has the application been recorded centrally in accordance with procedures?	Yes / No
Comments:	
2. Is there sufficient detail to establish whether surveillance is necessary and proportionate?	Yes / No
Comments:	
3. Is the Authorising Officer correct (ie on approved list or Chief Executive / Deputy Chief Executive if a juvenile or vulnerable person)?	Yes / No
4. If the surveillance is to be carried out, has approval been obtained from a Justice of the Peace, where appropriate?	Yes / No / N/A
Comments:	
5. a) Was a renewal necessary?	Yes / No / N/A
b) If yes , was the correct renewal form completed and judicial approval sought?	Yes / No / N/A
c) If a CHIS application, is there evidence of a review?	Yes / No / N/A
Comments:	
6. a) Was a cancellation necessary?	Yes / No / N/A
b) If yes , was the cancellation form completed?	Yes / No / N/A
Comments:	
7. Are there any errors to be reported to the Office of Surveillance Commissioner?	Yes / No
Comments:	
8. General comments:	

Regulation of Investigatory Powers Act (2000)

Document Control

Document owner:	Chief Corporate Solicitor
Document number:	Version 2
Document category:	Policy
Document location:	The Hub
Issued by:	Chief Corporate Solicitor
Last edited:	January 2016

Approved By:

Name	Date
Corporate RIPA Group	
Corporate Leadership Team	
Audit Committee	