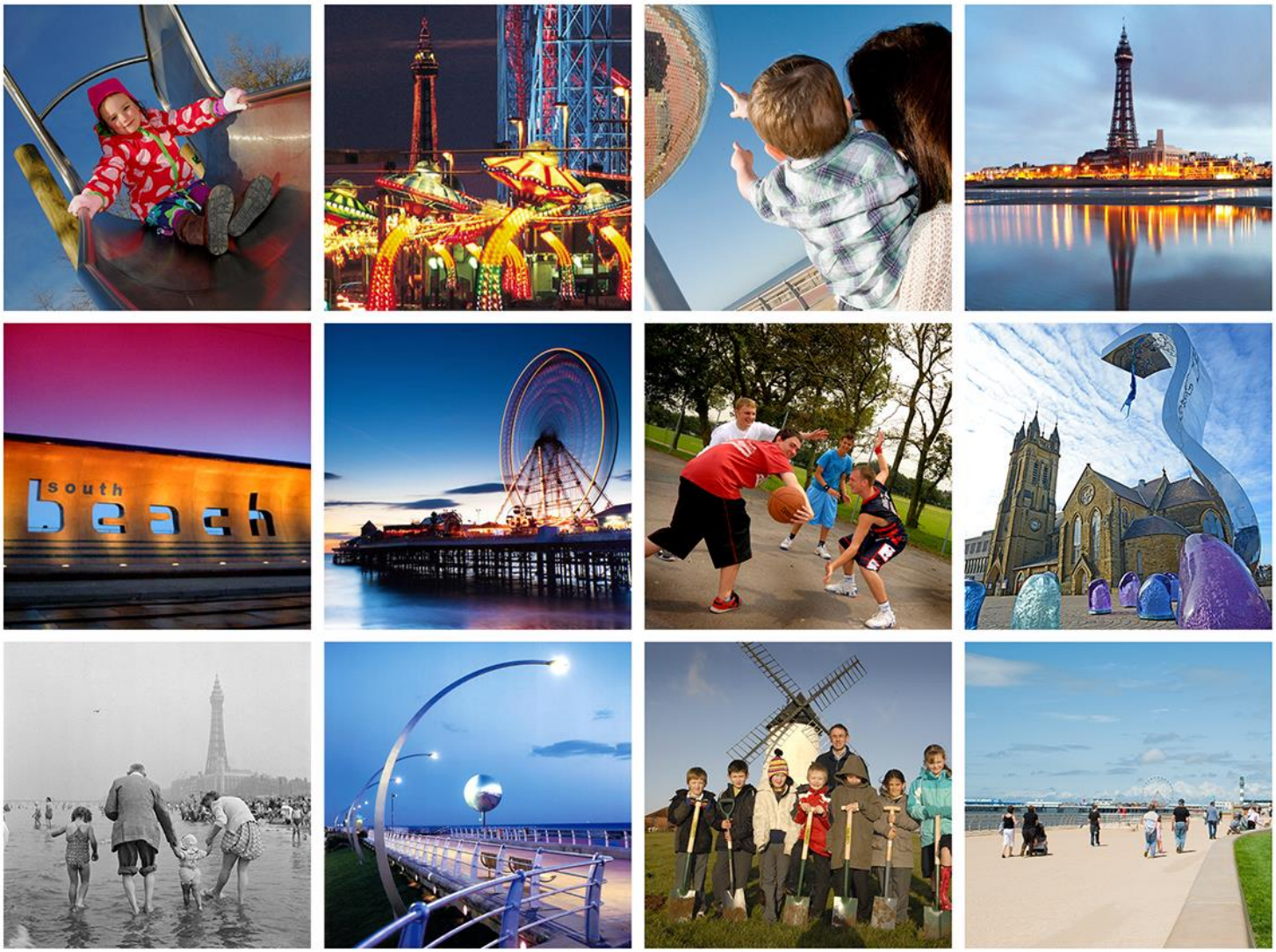
Appendix 6(a)

Regulation of Investigatory Powers Act Policy and Guidelines

Blackpool Council



Contents

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
- SOC 1 Social Media ID
- SOC 2 Social Worker surveillance

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

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!

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 Act also extends to any wholly owned Companies where the local authority acts as the appropriate body for RIPA applications and authorisations. Companies are not permitted to undertake covert surveillance without seeking the necessary advice and approval from the Council as the responsible authority. This protects both the Council and the Company 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.

2.4 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

2.5 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.

2.6 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.

2.7 Each relevant Director 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).

2.8 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".

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

2.10 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.

2.11 Deciding when authorisation is required involves making a judgement. Paragraph 4.4 and those immediately following 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 Head of Legal.

Consequences of not following RIPA

2.12 Section 27 of RIPA provides that surveillance shall be lawful for all purposes if authorised and conducted in accordance with an authorisation granted under RIPA.

2.13 Lawful surveillance is exempted from civil liability.

2.14 Although not obtaining authorisation does not make the authorisation unlawful per se, it does have some consequences:

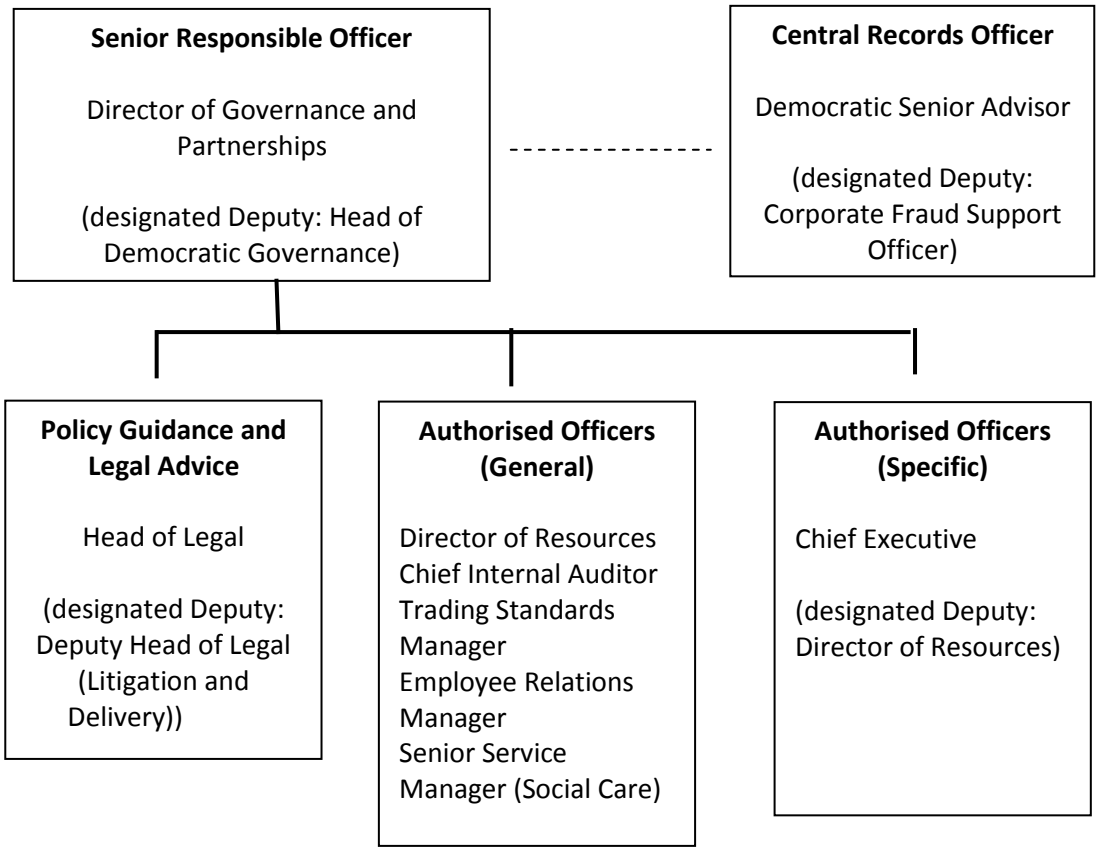
- Evidence that is gathered may be inadmissible in court;
- The subjects of surveillance can bring their own proceedings or defeat proceedings brought by the Council against them on human rights grounds i.e. we have infringed their rights under Article 8;
- If a challenge under Article 8 is successful the Council could face a claim for financial compensation;
- A complaint could be made to the Office of Surveillance Commissioners; and
- The Government has also introduced a system of tribunal. Any person who believes that their rights have been breached can have their complaint dealt with by way of a tribunal.

The Surveillance Commissioner

2.15 The Government has appointed a Surveillance Commissioner to review the way in which public authorities implement the requirements of RIPA. The Commissioner has a wide range of powers of access and investigation. The Council will receive periodic visits from the Office of the Surveillance Commissioners. They will check to see if the Council is complying with RIPA and it is important that the Council can show it complies with this Guide and with the provisions of RIPA.

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:



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 Head of Legal 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 Head of Legal 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 for these purposes (Director of Resources).

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.

4. Directed Surveillance

4.1 <u>What is meant by Surveillance?</u>

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 <u>When is surveillance directed?</u>

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 Head of Legal.

(v) The Council is not empowered to carry out intrusive surveillance

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.

5. Covert use of Human Intelligence Source (CHIS)

5.1 A person is a Covert Human Intelligence Source if:

(i) 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 ii) or iii)
(ii) they covertly use 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.

5.2 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.

5.3 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, therefore if in doubt obtain authorisation and judicial approval.

5.4 Below are examples of when a Covert Human Intelligence Source (CHIS) may or may not be needed:

Example One
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 the Local 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 Two
In similar circumstances, intelligence suggests that a shopkeeper will sell alcohol to juveniles from a room at the back of the shop, providing he has got to know them first and trusts them. Therefore, the Local Authority decides to deploy its operative on a number of occasions, to befriend the shopkeeper and gain his 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.

Example Three
A member of the public is asked by a member of the Local 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.

Example Four
A member of the public volunteers a piece of information to a member of a Local Authority regarding something he has witnessed in his neighbourhood. The member of the public would not be regarded as a CHIS. He/ She is not passing information as a result of a relationship, which has been established or maintained for a covert purpose.

6. Surveillance outside of RIPA

6.1 Amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 mean that a Local Authority can now only grant an authorisation under RIPA where the Local Authority is investigating criminal offences which attract a maximum custodial sentence of at least six months or criminal offences relating to the underage sale of alcohol or tobacco. However, there may exceptional circumstances where there is a necessity for the Council to undertake surveillance, which does not meet the criteria to use the RIPA legislation such as in cases of serious disciplinary investigations, or in the case of anti-social behaviour offences, or social media surveillance which do not attract a maximum custodial sentence of at least six months imprisonment for covert operations.

6.2 There are also occasions where Social workers use social media surveillance to determine whether or not a child is in need of protection, usually for short periods of

up to three weeks. Under this policy, social workers will be exempted from the full rigours of the RIPA regime for these short periods and instead they will be required to fill out a simple form for this limited activity. The full details of this policy are listed in Section 10 Social Media.

6.3 The Office of Surveillance Commissioners Procedures and Guidance 2011 states that it is prudent to maintain an auditable record of decisions and actions to use covert surveillance without the protection of RIPA and that such activity should be regularly reviewed by the Senior Responsible Officer. The Senior Responsible Officer will therefore maintain an oversight of non RIPA surveillance to ensure that such use is compliant with Human Rights legislation. The Central Records Officer will maintain a central record of non RIPA surveillance.

6.4 As part of the new process of formally recording and monitoring non RIPA surveillance, a non RIPA surveillance application form (see Appendix 4) should be completed and authorised by an Authorising Officer.

6.5 The Council must still meet its obligations under the Human Rights Act and any surveillance outside of RIPA must still be necessary and proportionate having taken account of the intrusion issues. The decision making process and the management of such surveillance must be well documented.

6.6 There is also a requirement for the Council's Senior Responsible Officer to regularly monitor surveillance outside of RIPA. Therefore, before surveillance is undertaken on any new activity, advice must be sought from the Head of Legal.

6.7 The Human Rights Act means that the Council by law has to respect the rights of everyone. In particular, Article 8 guarantees everyone the right to respect for their private and family life, their home and correspondence. This right can only be interfered with when the interference is in accordance with the law and necessary. RIPA provides the framework for public authorities to carry out surveillance and the lawful means whereby rights can be infringed by the Council.

7. Authorisations, renewals, duration and judicial approval

7.1 The Conditions for Authorisation

Directed Surveillance

7.1.1 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.

7.1.2 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

(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.

7.1.3 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.

7.1.4 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.

7.1.5 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.

7.1.6 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.

7.1.7 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.

7.1.8 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.

7.1.9 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.

7.1.10 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.

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

<u>Covert Use of Human Intelligence Sources</u>

7.1.12 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

(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.

7.1.13 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.

7.1.14 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.

7.1.15 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.

7.2 Requirements of the 2000 Act

7.2.1 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.

7.2.2 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

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'.

7.2.3 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.

7.2.4 The key signature on the application is that of the Authorising Officer on the authorisation and this must be handwritten. The original "wet signed" form must be lodged with the Central Records Officer.

7.2.5 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.

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

7.2.7 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.

7.2.8 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.

7.2.9 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.

7.2.10 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:

- 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).

7.2.11 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 Director of Resources (acting as Deputy to the Chief Executive for this purpose).

7.2.12 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.

7.2.13 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.

<u>Factors to Consider</u>

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

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

7.2.16 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.

7.2.17 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

7.2.18 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

7.2.19 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 Director of Resources in his absence) where confidential information or matters subject to legal privilege are likely to be acquired.

7.2.20 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.

7.2.21 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 doubt as to whether the material is confidential, advice should be sought from the Head of Legal 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 Head of Legal) 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

7.2.22 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.

7.2.23 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.

7.2.24 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 Head of Legal 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

7.2.25 Authorising Officers are reminded of the guidance relating to the retention and destruction of confidential material as described in paragraph 7.2.21.

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

7.2.27 Authorising Officers must ensure that the relevant details of each authorisation are sent to the Senior Responsible Officer as described in this Policy and Guidelines (Section 13).

7.2.28 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.

7.2.29 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 Head of Legal.

Review and Cancellation of Authorisations

7.2.30 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.

7.3 The Use of Covert Human Intelligence Sources – Employees

7.3.1 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.

7.3.2 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.

7.3.3 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.

7.3.4 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.

8. Specific Areas where RIPA needs to be considered.

Test Purchases

8.1 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, an authorisation for directed surveillance will be required. If recording equipment is not worn then the non-RIPA process must be followed (see section 6). In all cases, a prior risk assessment is essential in relation to a young person.

8.2 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

8.3 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

8.4 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.

8.5 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 tends 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 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.

9. CCTV Systems

9.1 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.

9.2 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.

9.3 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.

9.4 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.

10. Social Media

10.1 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.

10.2 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.

10.3 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.

10.4 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 the Senior Responsible Officer (or their representative) once they have been approved by an Authorising Officer. The Central Records Officer will retain this form. The Senior Responsible Officer will then maintain oversight that these arrangements are appropriate.

10.5 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). This authorisation must be retained by the Central Records Officer.

10.6 Social workers use social media surveillance to determine whether a child is in need of protection. It is used for short periods of up to three weeks. It is generally understood that if social workers were required to fill out forms that mirror the RIPA regime the complexity of the exercise and the time that it would take would deter such activity in most cases. This would mean that child abuse would go undetected in a large number of cases.

10.7 The overall purpose of the RIPA regime is to enable surveillance to take place where necessary in a manner that is proportionate to the risk. It also requires balancing the intrusion of privacy against the need to investigate crime or in this instance the protection of children or vulnerable adults. With that objective in mind, under this policy social workers are exempted from the full rigours of the RIPA regime for short periods of surveillance. Instead they will be required to fill out a simple form, which will extend for a period of no more than three weeks.

10.8 This form will be signed off by the Senior Service Manager (Social Care) or the Head of Adult Social Care (as appropriate) and lodged with the Central Records Officer. In the absence of the Senior Service Manager (Social Care), a Service Manager from a different team to the Social Worker who is conducting the surveillance will sign off the forms; the form can be found at Appendix 4. Any periods of surveillance longer than three weeks will require the use of the standard RIPA forms, which will be amended to reflect that fact that surveillance is outside the RIPA regime. The short authorisation procedure will include a form of assessment. An essential part of the assessment will be a determination of the child protection/ adult social care risk. It will involve asking questions such as, how serious is the nature of the risk and how likely is it to materialise? The level of intrusion or deception should also be taken into the equation.

10.9 Use of third parties who are known to the family for the purpose of accessing social media sites or asking questions is likely to engage the procedure for use of a covert human intelligence source. The short authorisation procedure is not suitable for this activity. This procedure is also not suitable for any surveillance that is likely to obtain confidential information.

11. Tracking Devices

11.1 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.

11.2 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

12. 'Drive by' Surveillance

12.1 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.

13. Noise Monitoring Equipment

13.1 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.

14. Central Register of Authorisations

14.1 The 2000 Act requires a central register of all authorisations and judicial approvals to be maintained. The Senior Responsible Officer maintains this register

14.2 Whenever an authorisation is granted the Authorising Officer must arrange for the following details to be forwarded in hard copy to the Senior Responsible Officer and will be retained by the Central Records Officer. (An 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.

14.3 If the authorisation is subsequently renewed or cancelled the following must be provided in hard copy to the Senior Responsible Officer and retained by the Central Records Officer.

14.4 The forms on the Appendices to this Policy must be used at all times.

14.5 It is each Department's responsibility to forward all applications to the Senior Responsible Officer 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 Senior Responsible Officer, 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.

14.6 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.

14.7 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 there representative) who will maintain a record of decisions and actions. Such activity will be regularly reviewed by the Senior Responsible Officer.

14.8 All surveillance equipment owned by the Council is also logged on a central register maintained by the Central Records Officer. When applying for authorisation the applicant should cross-reference the equipment deployment records and the relevant authorisation.

15. Retention

15.1 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.

15.2 All records held by the Departments should be disposed of in an appropriate manner (e.g. shredded).

15.3 Authorising Officers, through the relevant data controller, should ensure compliance with the appropriate data protection requirements under the Data Protection Act 1998 (or any subsequent legislation), the Council's Corporate Retention Schedule and the departmental practices is to take place for the secure handling and storage of materials.

16. Supporting information, Codes of Practice and Forms

16.1 Staff should refer to the Codes of Practice produced in the appendices to this Policy for supplementary guidance.

16.2 The relevant Codes of Practice, Forms, and sample completed forms are available in the RIPA Section of the Council's Intranet (The Hub).

16.3 Any queries relating to RIPA or this document should be addressed in the first instance to the Senior Responsible Officer or the Head of Legal.