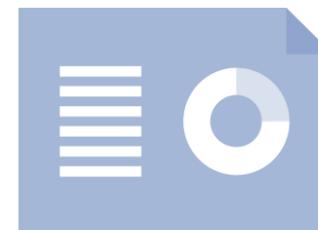


Blackpool Council

Follow-up data protection audit report

April 2022

Executive summary



Background

The Information Commissioner is responsible for enforcing and promoting compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA18) and other data protection legislation. Section 146 of the DPA18 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA18 allows the ICO to carry out consensual audits.

The ICO is an independent, proportionate regulator and sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach. High standards of personal data protection compliance help organisations innovate and deliver great services by building trust with the public. The ICO's expertise and consistent approach to regulation provides certainty enabling organisations to feel confident to use personal data responsibly, innovate and support economic growth.

Blackpool Council (BC) agreed to a consensual audit by the ICO of its processing of personal data. An introductory telephone meeting was held on 22 February 2021 with representatives of BC to discuss the scope of the audit.

The purpose of the audit is to provide the Information Commissioner and BC with an independent assurance of the extent to which BC, within the scope of this agreed audit, is complying with data protection legislation.

A desk based review of selected policies and procedures and remote telephone interviews were conducted from 20 April 2021 to 22 April 2021 and covered the following scope areas:

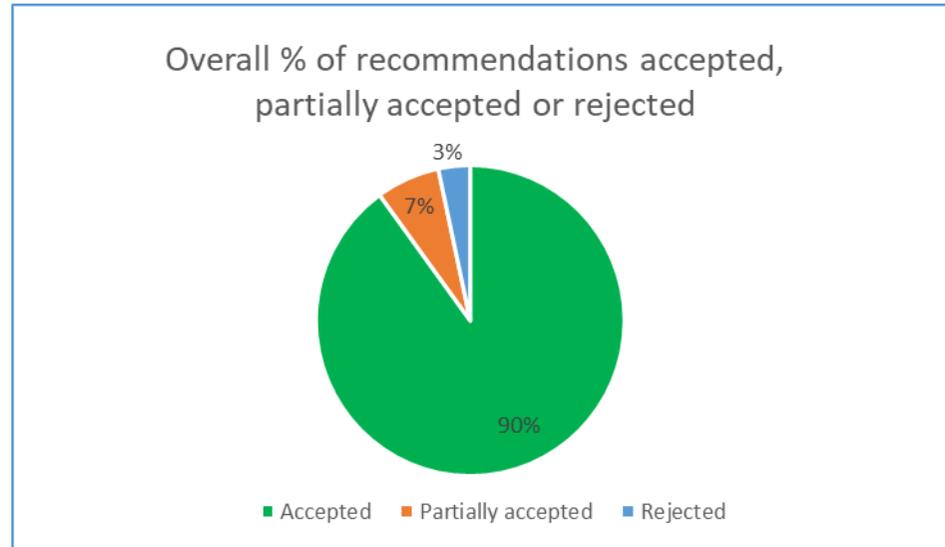
Scope Area	Description
Governance & Accountability	The extent to which information governance accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor data protection compliance to both the GDPR and national data protection legislation are in place and in operation throughout the organisation.
Information Security (Security of Personal Data)	There are appropriate technical and organisational measures in place to ensure the confidentiality, integrity and availability of manually and electronically processed personal data.
Freedom of Information (FOI)	The extent to which FOI accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor compliance are in place and in operation throughout the organisation.

Where weaknesses were identified recommendations were made, primarily around enhancing existing processes to facilitate compliance with data protection legislation.

30 recommendations were made in the original audit report. In order to assist BC in implementing the recommendations each was assigned a priority rating based upon the risks that they were intended to address. The ratings were assigned based upon the ICO's assessment of the risks involved.

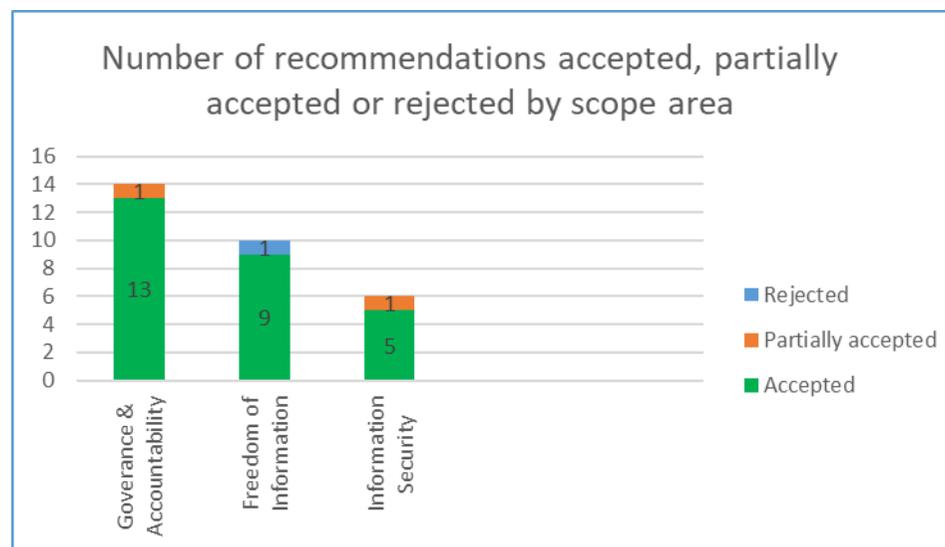
BC responded to these recommendations positively, agreeing to formally document procedures and implement further compliance measures.

The following chart summarises BC's response to the recommendations made.



A pie chart showing the overall percentage of recommendations accepted, partially accepted or rejected.

The pie chart above shows that overall, 90% of recommendations have been accepted, 7% have been partially accepted and 3% have been rejected.



A bar chart showing the number of recommendations accepted, partially accepted or rejected by scope area

The bar chart above shows that for the Governance and Accountability scope, 13 recommendations have been accepted and 1 has been partially accepted.

For the Freedom of Information scope, 9 recommendations have been accepted and 1 has been rejected.

For the Information Security scope, 5 recommendations have been accepted and 1 has been partially accepted.

Follow-up process

The objective of a follow-up audit assessment is to provide the ICO with a level of assurance that the agreed audit recommendations have been appropriately implemented to mitigate the identified risks and thereby support compliance with data protection legislation and implement good practice.

For all Urgent and High priority recommendations made in the original audit report, BC are required to provide an update on the actions they have taken with supporting documentation to evidence progress.

For all Medium and Low priority recommendations made in the original audit report, BC are required to provide an update on the actions they have taken.

The updated Action Plan should be signed off at Board Level.

Follow-up audit summary

A desk based follow-up took place in April 2022 to provide the ICO and BC with a measure of the extent to which BC had implemented the agreed recommendations. In all the scope areas covered by the audit we are pleased to note that all recommendations have been completed.

Key follow-up audit findings

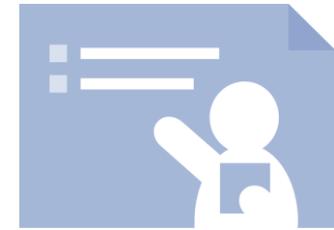
Main improvements include:

- BC have increased their resources by recruiting a new Information Rights Assistant to ensure that the IG team has sufficient resources proportionate to the number and complexity of SAR requests it receives. This will ensure that a higher proportion of SAR requests are responded to within statutory timescales;
- BC have developed new KPI's to ensure they have sufficient oversight of their management of records., including what percentage of records are destroyed in line with the corporate retention schedule;
- BC have documented the procedure to authorise the use of FOI exemptions or exceptions and ensure the authorisations are recorded. This will demonstrate BC's use of exemptions or exceptions is subject to proper approval;
- BC have included key FOI/EIR elements in their training to ensure that staff knowledge and awareness is maintained. This will provide BC with more assurance that staff will operate within internal and legislative requirements.

Follow-up audit conclusion

The follow-up is now complete, BC has completed all the actions agreed in the original audit.

Credits



ICO Auditor

James Donnelly – Lead Auditor

Thanks

The ICO would like to thank Jonathan Pickup, Data Protection Officer for their help in the audit follow up engagement.

Distribution List

This report is for the attention of Jonathan Pickup, Data Protection Officer.

Disclaimer

The matters arising in this report are only those that came to our attention during the course of the follow up audit and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rest with the management of Blackpool Council.

We take all reasonable care to ensure that our follow up audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.

This report is solely for the use of Blackpool Council. The scope areas and controls covered by the original audit were tailored to Blackpool Council and, as a result, this report is not intended to be used in comparison with other ICO follow up audit reports.