Bury Metropolitan Borough Council

Data protection audit report

July 2021

Information Commissioner's Office

Executive summary

Audit Methodology

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 sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach.

Bury Metropolitan Borough Council (BMBC) agreed to a consensual audit by the ICO of its processing of personal data. An introductory telephone meeting was held on 23 March 2021 with representatives of BMBC to discuss the scope of the audit.

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

The scope areas covered by this audit are determined following a risk based analysis of BMBC processing of personal data and Freedom of Information requests. The scope may take into account any data protection issues or risks which are specific to BMBC, identified from ICO intelligence or BMBC's own concerns, and/or any data protection issues or risks which affect their specific sector or organisations more widely. The ICO has further tailored the controls covered in each scope area to take into account the organisational structure of BMBC, the

nature and extent of BMBC's processing of personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to BMBC.
It was agreed that the audit would focus on the following area(s)

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 UK GDPR and national data protection legislation are in place and in operation throughout the organisation.
Information Security	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	The extent to which FOI/EIR accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor compliance are in place and in operation throughout the organisation.

Audits are conducted following the Information Commissioner's data protection audit methodology. The key elements of this are normally a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

However, due to the outbreak of Covid -19, and the resulting restrictions on travel, this methodology was no longer appropriate. Therefore, BMBC agreed to continue with the audit on a remote basis. A desk based review of selected policies and procedures and remote telephone interviews were conducted from 22 June to 24 June 2021 The ICO would like to thank BMBC for its flexibility and commitment to the audit during difficult and challenging circumstances.

Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection and freedom of information legislation. In order to assist

BMBC in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. BMBC'S priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

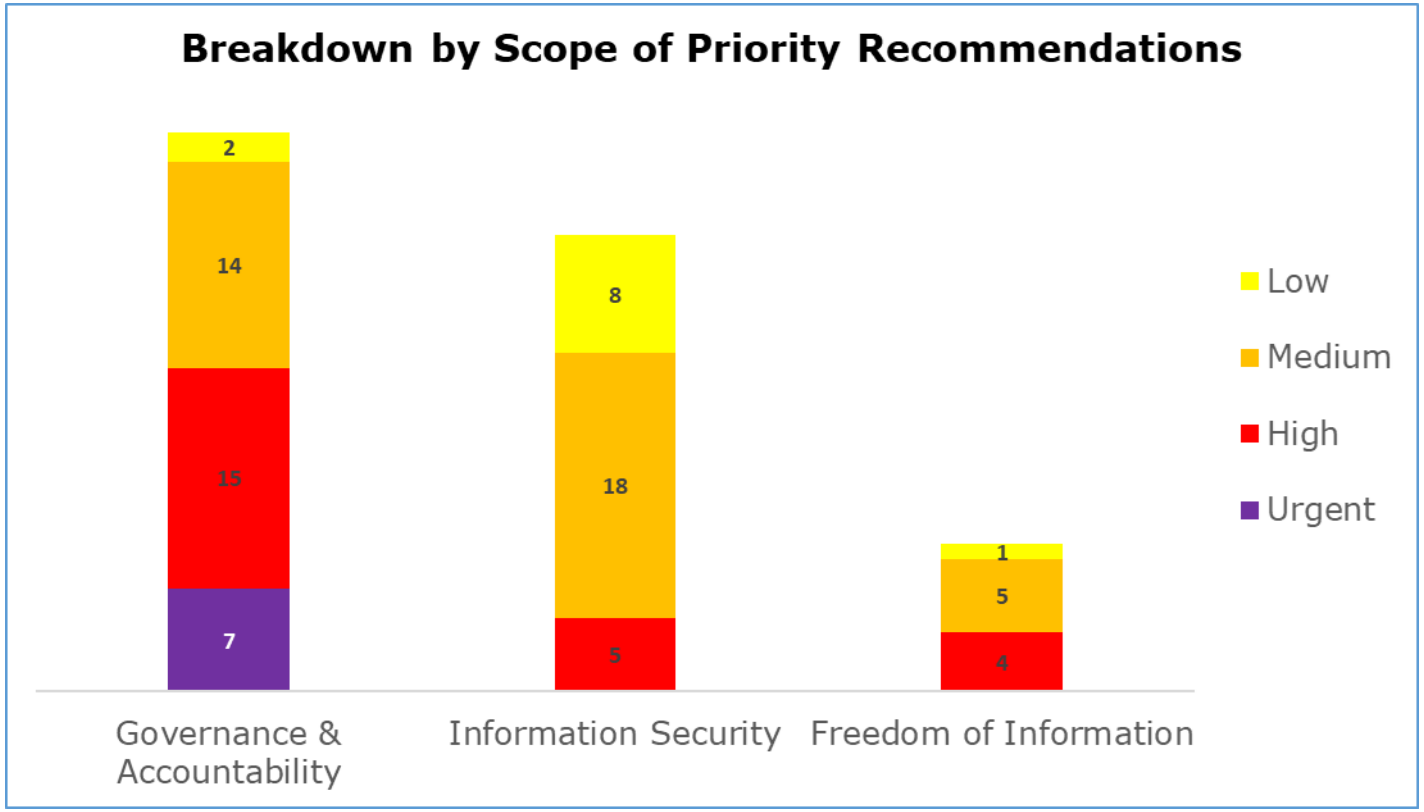
Audit Summary

Audit Scope area	Assurance Rating	Overall Opinion
Governance & Accountability	Limited	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Information Security	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Freedom of Information	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering freedom of information compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with freedom of information legislation.

*The assurance ratings above are reflective of the remote audit methodology deployed at this time and the rating may not necessarily represent a comprehensive assessment of compliance.

Priority Recommendations

A bar chart showing a breakdown by scope area of the priorities assigned to the recommendations made.



The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Governance & Accountability has seven urgent, 15 high, 14 medium and two low priority recommendations
- Information Security has five high, 18 medium and eight low priority recommendations
- Freedom of Information has four high, five medium and one low priority recommendations

Areas for Improvement

BMBC does not currently maintain a central log of its lawful bases for processing, meaning there is no oversight on whether the appropriate lawful basis is being used. BMBC should establish a central log of lawful bases, including details of any law, statute, or other obligation for that processing.

The Records of Processing Activities (RoPA) held by BMBC does not include certain categories of information required by the UK GDPR. BMBC should ensure that its RoPA is updated to include all details specified by the legislation.

BMBC does not have a Legitimate Interests Assessment (LIA) in place for the processing it carries out under the lawful basis of Legitimate Interest. BMBC should undertake an LIA on this processing to ensure it has adequately balanced its interests against the rights and freedoms of the data subject.

BMBC should gain assurance from suppliers that they will notify BMBC within a reasonable timeframe of any information security breaches or personal data breaches. All breaches should be notified to a nominated person.

BMBC should separate out the key elements of FOI/EIR legislation from the existing Data Protection eLearning module to create a new FOI module. Use the new module for mandatory FOI induction and refresher training for all staff.

A specialist training programme should be created for all those staff with responsibility for responding to FOI/EIR requests. The training should be recorded and refreshed on a regular basis.

BMBC should review the existing FOI pages on the council web site to demonstrate and ensure compliance with current guidance whilst ensuring the benefits gained from the web request form are not diminished.

Best Practice

BMBC have integrated communications around information governance into weekly executive emails, ensuring data protection matters are visible to all levels of staff.

Departments hold a library of responses to frequent FOI/EIR requests to reduce workload, reduce response times and capitalise on any effort already expended on similar requests.

BMBC has metacompliance software in place to ensure all staff have read and completed the Personal Commitment Statement. The statement outlines key information security requirements that staff must follow.

Disclaimer

The matters arising in this report are only those that came to our attention during the course of the 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 Bury Metropolitan Borough Council.

We take all reasonable care to ensure that our 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 an exception report and is solely for the use of Bury Metropolitan Borough Council. The scope areas and controls covered by the audit have been tailored to Bury Metropolitan Borough Council and, as a result, the audit report is not intended to be used in comparison with other ICO audit reports.