Bury Metropolitan Borough Council

Follow-up data protection audit report

April 2022

Information Commissioner's Office

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.

Bury Metropolitan Borough Council (BMBC) agreed to a consensual audit by the ICO of its processing of personal data and Freedom of Information Act (FOIA) requests.

Due to Covid -19 events, the original audit took place via document review and remote interviews between 22 June to 24 June 2021 and covered the following 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 UK 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/EIR accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor compliance are in place and in operation throughout the organisation

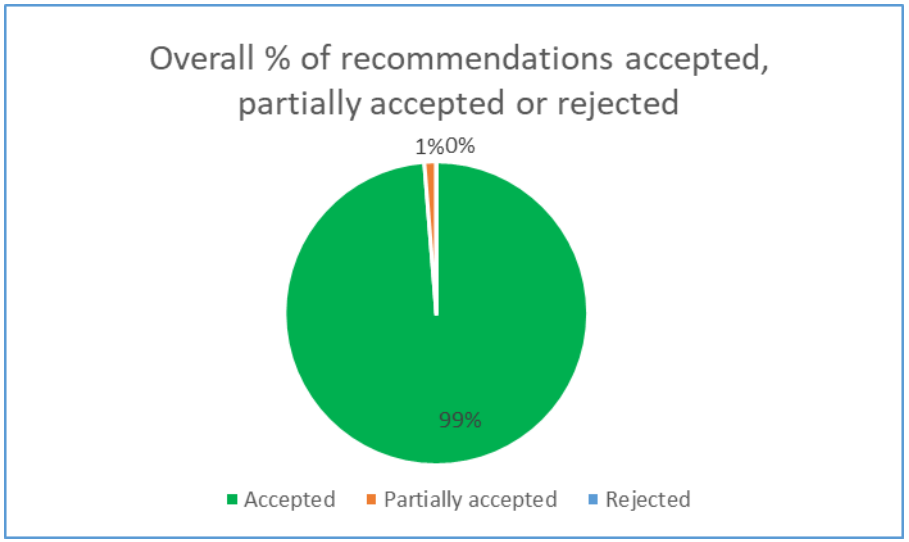
Where weaknesses were identified recommendations were made, primarily around enhancing existing processes to facilitate compliance with the DPA18 and FOIA.

79 recommendations were made in the original audit report. In order to assist BMBC 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.

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

The following charts summarise BMBC'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, 99% of recommendations have been accepted, 1% have been partially accepted and 0% have been rejected.

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 and freedom of information legislation and implement good practice.

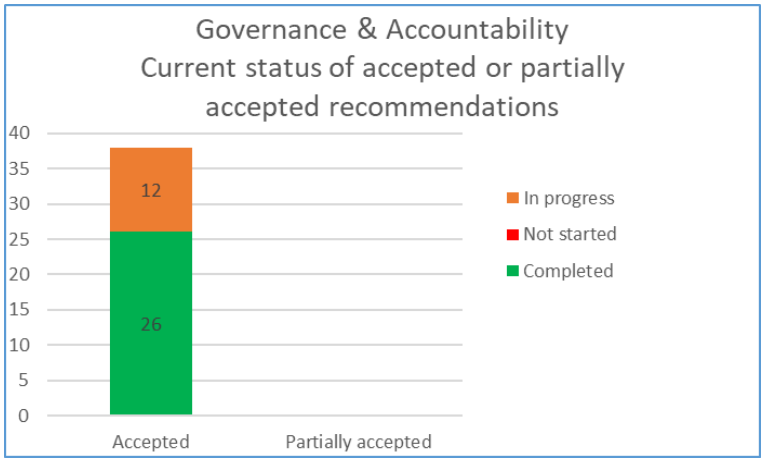
For all Urgent and High priority recommendations made in the original audit report, BMBC are required to provide an update on the actions they have taken with supporting documentation to evidence progress.

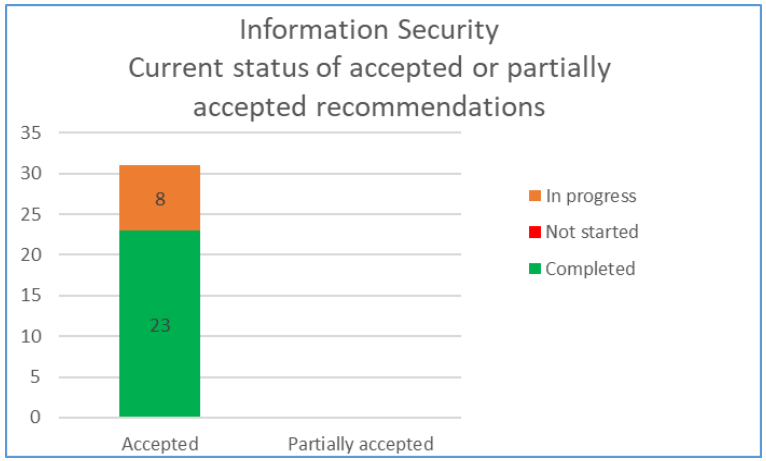
For all Medium and Low priority recommendations made in the original audit report, BMBC are required to provide an update on the actions they have taken.

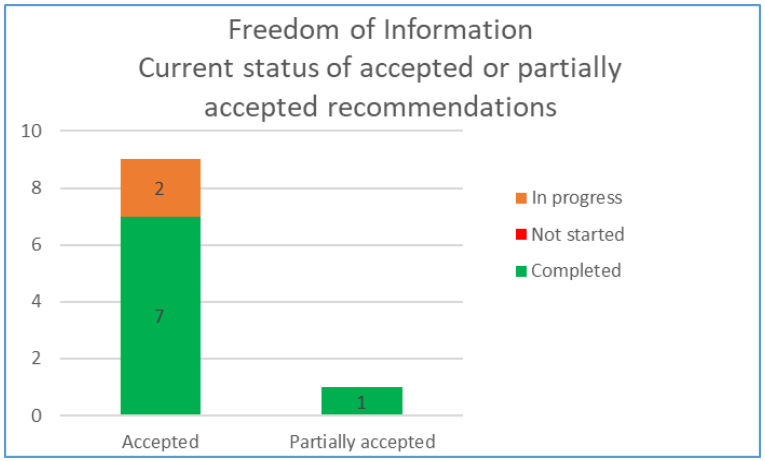
The updated Action Plan should be signed off at Board Level.

Follow-up audit summary

A desk based follow-up took place in April 2022 to provide the ICO and BMBC with a measure of the extent to which BMBC had implemented the agreed recommendations. The following charts show a summary of progress to date.







- In the Governance and Accountability scope area we are pleased to note that 26 of the accepted recommendations have been completed, however 12 remain still in progress.
- In the Information Security scope area we note that 23 of the accepted recommendations have been completed and eight remain still in progress.
- In the Freedom of Information scope area there are seven accepted recommendations and one partially accepted recommendation which have been completed. Only two remain still in progress.

There are several recommendations where ICO's opinion as to their status has differed from BMBC's opinion.

Where the ICO has assessed actions as still in progress and BMBC have marked these actions as completed:

Urgent and High priority actions (see main risk areas still outstanding below for details): a.7, a.19, a.20, b.11, b19.

Medium and Low priority actions:

a.13 – Policies are reviewed every two years, however there is no specific compliance section within the Policy Template explaining how monitoring of compliance with the policy will be carried out.

b.7 - Although evidence was provided to suggest that a high level monitoring of the risk of outdated infrastructure, data centre, applications and programmes is managed on the Information Governance (IG) Risk Register, there is no evidence that a written assessment methodology is in place to manage and list the risks associated with individual outdated IT Hardware and software. It was reported that IT apply the HAZID/HAZOP risk assessment methodologies to risk assess IT projects, software and infrastructure. BMBC are yet to decide whether to purchase a tool to manage the risk assessment process.

Where the ICO has assessed actions as completed and BMBC has marked these actions as still in progress:

b.22 - Auto screen lock timing has been reviewed and has been adjusted. The IT Security Policy indicates that PCs will lock after 20 minutes if unattended or inactive.

Key follow-up audit findings

Main improvements include:

- An IG Manager has been allocated and acts as BMBC's Data Protection Officer (DPO). The role has been documented in a detailed job description. This should help to avoid any conflict of interests. A fixed term resource has also been allocated to assist the IG Manger (a.1).
- A large network of IG Champions has been reinstated since November 2021. The group meets monthly. Updates from the meetings are provided to Information Governance Steering Group (IGSG). This should help BMBC embed its compliance of data protection and FOI across the Council (a3).
- An updated Risk Management Strategy has been implemented. An IG Risk Register has been developed. Evidence has been provided that IG high level themes are monitored at corporate level (a.4).
- An Appropriate Policy Document has been created and approved by IGSG (a.6).
- IG Key Performance Indicators (KPIs) have been set and reported against monthly to IGSG. Some KPIs have been reported to the Audit Committee on a monthly basis (a.16)
- Contracts have been updated to include the requisite UK GDPR clauses. Compliance around the contracts register is reported quarterly to IGSG. Contract monitoring is in place and the DPO reviews key contracts annually (a.16).
- A Legitimate Interest Assessment has been completed setting out the legitimate interests for processing of personal data for HR purposes. This was completed in October 2021 (a.23).
- The DPIA checklist, template and guidance has been reviewed and updated. DPIA screening needs to be completed before the outset of all projects (a.31, a32, a33, a.34 and a.35)

- An updated IG Incident Procedure has been approved by IGSG. It was reported that reporting of IG Incidents process is reinforced through the IG mandatory training. Training statistics are reported to IGSG and the Audit Committee. (a.36 a & b).
- The breach log has been updated to include a section for recording any actions taken and points of learning from incidents. A monthly report on personal data breaches is provided to IGSG by the DPO (a.36.c).
- The Information Security (IS) Policy and IT Security Policy have been updated to include the requisite version control information (b.1).
- A review of all contracts has been completed to ensure they include the expected IG clauses. All contracts are checked by the DPO to ensure they contain the requisite clauses around personal data breach notification by the processor within a specific timescale. Contactors are expected to follow the IS Policy which also outlines personal data breach reporting guidance (a.15 and b.28).
- The IG Incident Procedure includes information on how and when the ICO and data subjects need to be notified (b.31)
- All FOI and EIR guidance has been reviewed and updated and is available on the intranet. FOI and EIR requests will now be administered through the newly established Business Support Service. This will allow greater consistency of responses and ensure deadlines are met (c.1 and c.4).
- FOI training needs have been reviewed and training content refreshed. FOI training is part of BMBCs mandatory training suite. This training is refreshed annually by all staff (c.3 and c.8).

Main risk areas still outstanding:

- A policy template has been created which includes the expected document control information. An IG Policy Schedule has been created. Some polices have been reviewed, but some information has not been populated for example the date of next review. There is also no information provided on whether ICT policies have been reviewed or not (a.7)

- A training needs analysis has been created for all IG training. This includes training for specialist IG roles. The Caldicott Guardian has completed relevant training. However other specialist training is still at the commissioning stage and is yet to be completed (a.10).
- A lot of work has gone into updating the Record of Processing Activities (ROPA), which is now a detailed document. A process for maintaining the ROPA has been created and rolled out. Information Asset Owners and Information Asset Managers have received training around their responsibilities linked to the ROPA. The ROPA contains the majority of the information expected under UK GDPR Article 30.1 apart from (g) 'a general description of the technical and organisational security measures referred to in Article 32(1)'. In order to ensure full compliance with UK GDPR Article 30. BMBC will need to record its technical and organisational measures used to protect the personal data it is processing (a.19).
- There is a column in the ROPA where the purpose of the processing is detailed. Where legal basis has been recorded, some entries record a clear statutory basis but other entries do not. Where public interest has been recorded as a lawful basis, the public interest activity has not always been clearly defined (a.20).
- USB storage devices are no longer in use. BMBC are currently in the process of moving to Microsoft Device Management and encryption solution. It plans to put in place measures to prevent the reading of and writing to USB pen drives (b.11).
- The Agile Working Policy is referenced within the IT Security Policy. However there is no detailed process for granting and revoking access to buildings. Also, it has been reported that the DPO will request a spot check on a quarterly basis of staff access to buildings, however there is no evidence that these checks have been carried out as yet (b.19).
- Staff in Business Support Service are due to receive training on the new FOI and EIR request process (c.9).

Observations:

a.1. The DPOs role has been documented in a detailed job description (JD). It covers the majority of the tasks expected of the DPO within UK GDPR Articles 35, 35 and 37. However the JD doesn't reference the fact that

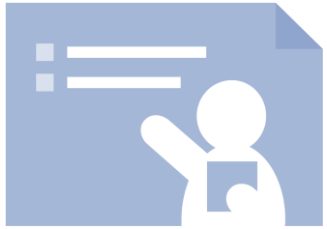
the DPO should act as the point of contact for the Regulatory Authority (the ICO) for any queries or complaints, where there may be a reportable personal data breach to ICO or where prior consultation with the ICO is required for high risk processing where risks cannot be sufficiently mitigated.

b.10.- It is reported that there is a form on the intranet that staff can complete to explain why they need to transport data outside of normal methods. This is signed off by a line manager. This process hasn't been referenced in the IS or IT Security Policies.

Follow-up audit conclusion

The follow-up is now complete, BMBC has made good progress towards completing the actions agreed in the original audit. Some outstanding actions exist, but meaningful progress is being made with the remaining actions to mitigate the risk of non-compliance.

Credits



ICO Auditor

Helen Oldham – Lead Auditor

Thanks

The ICO would like to thank Marcus Connor, Information Governance Manager and Data Protection Officer for their help in the audit follow up engagement.

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 Bury Metropolitan Borough 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 Bury Metropolitan Borough Council. The scope areas and controls covered by the original audit were tailored to Bury Metropolitan Borough Council and, as a result, this report is not intended to be used in comparison with other ICO follow up audit reports.