Classification Open	Item No.

Meeting:	Audit Committee
Meeting date:	30th September 2021
Title of report:	Information Governance – ICO Update & Q2 delivery Update
Report by:	Lynne Ridsdale – Deputy Chief Executive
Decision Type:	
Ward(s) to which report relates	All

Executive Summary:

Information Governance (IG) is the strategy or framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards, ensuring compliance with the relevant statutory and regulatory requirements. At its last meeting the Audit Committee received the Q1 update on IG activity and approved the Information Governance Framework through which these functions are discharged within the Council.

During Q2 the Council has prepared and delivered a consensual audit of IG practice form the industry regulator, the Information Commissioner's office. This report:

- sets out the findings of the ICO audit;
- provides a Q2 update to the Information Governance workplan;
- proposes an improvement plan for adoption, which will also form the work plan for Quarters 3 and 4 2021/22; and
- sets out the requirements for the 2021/22 Data Security Protection Toolkit (DSPT).

Key considerations

1.0 Introduction

1.1 This report is the update on Information Governance work completed during Quarter 2 of 2021/22. The report focusses on the preparation for and findings of a consensual audit undertaken during this time by the Information Commissioner's Office (ICO). The full report is appended.

2.0 Background

2.1 The Information Commissioner is responsible for enforcing and promoting compliance with data protection legislation. Article 58(1) of the UK General Data Protection Regulation (UK GDPR) states that the Information Commissioner's Office (ICO) has the power to carry out investigations in the form of data protection audits. Section 129 of the Data Protection Act 2018 (DPA 18) also provides provision to carry out consensual audits. Additionally, Section 146 of the DPA 18 allows the ICO, through a written "assessment notice", to carry out an assessment of compliance with the data protection legislation.

2.2 Bury Council agreed to a consensual audit by the ICO of its processing of personal data. This was originally scheduled for June 2020; however, this was paused in response to the Covid-19 pandemic and was subsequently re-scheduled for 22nd – 24th June 2021.

2.3 The primary purpose of the audit was to provide the ICO and Bury Council with an independent opinion of the extent to which Bury Council, within the scope of the agreed audit, is complying with data protection legislation.

2.4 A report has been provided to Bury Council which, along with a series of recommended actions, also reflected on areas of good practice.

3.0 ICO Audit Approach

3.1 The ICO audit was structured as an evaluation of three areas of IG activity:

- Information security
- Freedom of Information
- Governance and Assurance

3.2 The Audit involved:

- Desk top review of over 100 pieces of written evidence including staff training materials, leadership job descriptions, policies, procedures, staff guidance and records of processing activity

- Over 30 stakeholder interviews with a range of staff involved in information governance activity

3.3 To inform the Audit the Council provided a copy of the Council's Information Governance Framework and internal improvement plan, which includes the actions from the recent Internal Audit review.

4.0 ICO Audit Findings

4.1 The ICO report is provided at Appendix A. The summary opinion is provided below

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.

4.2 The audit also highlighted the following areas of 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

4.3 The summary areas for improvement were found to be:

- 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.

5.0 Improvement Plan

5.1 The ICO have made 78 recommendations across the three themes of the audit, which have also been categorised by level of priority as follows

	Urgent	**High**	**Medium**	**Low**	**Total**
Governance and Assurance	7	15	14	2	38
Information Security	-	5	18	8	31
Freedom of Information	-	4	5	1	10

5.2 The recommendations have been translated into a detailed improvement plan for delivery by the end of the 2021/22 financial year. The detailed plan, which is performance managed by the Information Governance Steering Group, is available for inspection. A synopsis of activity underway is as follows

By end August	• Resolve Legitimate Interest Assessment – HR • ROPA refreshed • Review responsibilities/resources for IG • Refresh & re-establish network IG champions • Risk management strategy approved

	• Individual rights policy & procedure drafted • IG Policies updated to reflect GDPR • Induction updated & systems access only granted once e-learning complete • Contacts reviewed re data processing • DPIA screening, template and log established
By end Sept	• Resolve IS responsibilities within ICT • Update agile policy re information security • PEN test and review PSN requirements • Update personal breach policy • policy document template & schedule approved, including Information Security • policy availability to non front line staff addressed • IG KPIs reviewed • IAR reviewed following ROPA refresh • ROPA review process agreed • Privacy notice log established • FOIA policy and procedure updated
By end Oct	• Review GDPR e-learning module • Update Information Security policy in full • Establish end use asset register • Port controls designed within Enterprise Agreement • Specialist role training delivered to IG leadership roles • Internal audit plan
By end Nov	• Process for reviewing systems access in place • Resolve information security within buildings including floor walks of office sites
By end Dec	• End user device policy in place • Starter/leavers process reviewed and induction updated • Plans in place for independent assurance of IG • Audit of consent processes and recording • Review PETS

6.0 Information Governance Update 2021/22 Quarter 2

6.1 The following updates are provided in respect to the overall work programme.

- **Data Security and Protection Toolkit**

The 2021/22 iteration of the Data Security and Protection Toolkit (DSPT) was formally released by NHS Digital at the end of August 2021.

This Toolkit is a self-assessment implemented all organisations accessing NHS patient data and provides assurance as to the level of best practice in terms of the processing, storage and transfer of patient data. This is reflected in the Information Standards Notice DCB0086 Amd 9/2019.

For the 2021/22 reporting period, the submission deadline has been confirmed as 30 June 2022. As with the previous 2020/21 DSPT, there is acknowledgement of the continuing pressures resulting from the Covid-19 pandemic and as such, the deadline has been extended beyond 31 March for the 2021/22 submission.

With the recent release of the 2021/22 requirements which include additions to previous years (attached at Appendix B), work is currently progressing to incorporate these actions into the comprehensive IG workplan.

- **Information Governance Framework**

The Information Governance Framework endorsed by the Audit Committee at the June 2021 meeting is undergoing implementation to evidence assurance of effective governance practices across all Council departments. Key updates are noted below:
Information Governance Steering Group – the Group has been established as detailed above and continue to supervise and monitor all work in relation to the delivery of the workplan.

- **Information Governance Delivery Group**

This Group held their first meeting on 8th September 2021 and have been tasked with the coordination and delivery of individual actions on the workplan. The constitution reflects direct reports of Information Asset Owners (IAOS) whose departments have specific actions assigned to them. As such, there is no defined membership as the colleague best placed to progress the task in question is invited to attend.

- **Information Governance Resource**

Following a review of available resource, an Information Governance and Risk Strategic Advisor has been engaged to provide leadership direction across both the Council and CCG on a part-time, fixed term basis until January 2022; additionally supporting the seconded IG Support Officer role.

- **Policy**

Existing Information Governance and Data Security policies have been refreshed and updated in accordance with ICO recommendations. The documents currently undergoing review and approval by the IGSG include, but are not limited to the following:

- Data Subject Rights Policy
- Anonymisation and Pseudonymisation Policy
- Data Quality Policy

- Confidential Waste Disposal Policy
- Data Protection Impact Assessment (DPIA) Policy

- **Standards, including Training**

Alternative E-Learning modules within the existing training platform covering Information Governance and Cyber Security have been reviewed against National Cyber Security and ICO guidance and assurance provided they meet requirements of the audit recommendations. Work continues to progress, having identified, and now reviewing appropriate training materials for specialised IG roles.

7.0 Recommendations

4.1 The Audit Committee is required to:

- Note the 2021/22 Quarter 2 Update provided;
- Note the findings of the ICO audit at Appendix A;
- Note the 2021/22 requirements of the Data Security and Protection Toolkit provided at Appendix B.

Other alternative options considered

None.

Community impact / Contribution to the Bury 2030 Strategy

Good Information Governance practices enables the Council to deliver its statutory requirements and therefore contributes across all the themes of the Bury 2030 Strategy.

Equality Impact and considerations:

24. *Under section 149 of the Equality Act 2010, the 'general duty' on public authorities is set out as follows:*

A public authority must, in the exercise of its functions, have due regard to the need to -

(a) *eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by or under this Act;*

(b) *advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it;*

(c) *foster good relations between persons who share a relevant protected characteristic and persons who do not share it.*

25. *The public sector equality duty (specific duty) requires us to consider how we can positively contribute to the advancement of equality and good relations, and demonstrate that we are paying 'due regard' in our decision making in the design of policies and in the delivery of services.*

Assessment of Risk:

The following risks apply to the decision:

Risk / opportunity	Mitigation
Without a robust framework in place to support good Information Governance practice, there is a risk that the Council may not comply with the duties set out in the General Data Protection Regulations (GDPR) 2018 or Data Protection Act leading to possible data breaches, loss of public confidence, reputational damage and prosecution / fines by the Information Commissioner	Approval and Implement of the Information Governance Framework Implementation of a comprehensive Information Governance work programme

Consultation: N/a

Legal Implications:

The report references the Council's statutory duties and obligations under the UK GDPR, Data protection Act 2018, FOIA and associated legislation and guidance. The Council has duties under this legislation in terms of accountability and compliance and must ensure it has appropriate policies and procedures in place. A Failure to ensure compliance could result in enforcement action by the ICO.

Legal advice and support will be required in terms of the action plan outlined in the report as well as ongoing DPO oversight and support.

Financial Implications:

With the exception of the procurement of appropriate training there are no direct financial implications arising from this report. However, there are implications in relation to a potential ICO fine if the Council had a data breach and the ICO found that we as an organisation were negligent.

Report Author and Contact Details:

Lynne Ridsdale – Deputy Chief Executive

l.ridsdale@bury.gov.uk

Background papers: N/A

Please include a glossary of terms, abbreviations and acronyms used in this report.

Term	Meaning
DFM	Data Flow Mapping
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSPT	Data Security and Protection Toolkit
EIR	Environmental Information Regulations 2004
FOIA	Freedom of Information Act 2000
GDPR	General Data Protection Regulations 2018
IAM	Information Asset Manager
IAO	Information Asset Owner
IAR	Information Asset Registers
ICT	Information Communication and Technology

IG	Information Governance
IS	Information Security
IGSG	Information Governance Steering Group
KPI	Key Performance Indicator
LIA	Legitimate Interest Assessment
NHS	National Health Service
PEN	Penetration Testing
PETS	People Equipment Technology and Services
ROPA	Record of Processing activity
SAR	Subject Access Request
SIRO	Senior Information Risk Officer