

Classification	Item No.
Open	

Meeting:	Audit Committee
Meeting date:	1 December 2022
Title of report:	Information Governance Update
Report by:	Lynne Ridsdale – Deputy Chief Executive
Decision Type:	For information
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 July 2022 meeting, Audit Committee received the first of the new-format report to demonstrate how Information Governance is integrated into the delivery of services in the Council.

This report highlights improvements in training compliance, performance at responding to requests for information and dealing with data breaches. While the overall trend shows an increasing awareness of information governance in the Council, it is essential that this momentum is continued. Areas of particular focus over the coming months will be around updating the RoPA and increasing training to managers.

Key considerations

1.0 Introduction

- 1.1 This report is to update Audit Committee on the Council's Information Governance activity up to the end of November 2022.
- 1.2 As mentioned in the report to the July committee meeting, this report now focuses on the Council's 'business as usual' performance in the delivery of Information Governance.

2.0 Background

- 2.1 Following the Information Commissioner's Office (ICO) virtual re-visit to the Council on 11-14 April 2022, it was recognised that the Council had made strong progress against the 79 recommendations made following the ICO's June 2021 initial review.
- 2.2 As a result, this has now allowed the Council to focus delivering its day-day information governance responsibilities.

3.0 Next Steps / Business As Usual

3.1 Communications

- 3.1.1 Information Governance updates continue to be issued as part of the weekly Corporate Communications.
- 3.1.2 There have also been separate presentations to senior managers' meetings.

3.2 Training

- 3.2.1 As previously reported, following the ICO's recommendations, the Council has enhanced its annual mandatory UK GDPR training module.
- 3.2.2 The percentage of staff with up to date training will vary during the year.
- 3.2.3 When the Data Security & Protection Toolkit (DSPT) was submitted in June 2022, over 95% of staff had completed this training.
- 3.2.4 At the time of the last report to Audit Committee, performance stood at 78%. Since then, there has been a considerable rush for officers to complete their training, with the most recent figure being 92% of all staff members having completed the training, representing 158 individuals. Work is underway to ensure the remaining members of staff complete their training over the next few weeks.

- 3.2.5 To supplement the mandatory training, additional briefings on avoiding and learning from data breaches have been provided to individual teams and services. Briefings on information governance and learning from staff awareness surveys (carried out as part of the DSPT submission) have been provided to senior managers.
- 3.2.6 During 2023, a module on Information Governance will also be included in the Management Development Programme.
- 3.3 Update of the Record of Processing Activities (RoPA)
- 3.3.1 Extensive work has already been carried out to update the RoPA since the time of the ICO's visit in 2021.
- 3.3.2 Work is continuing to make the RoPA a more up to date and robust document. While this work has not been as progressed as initially intended, this reflects the scope of the work required. At the completion of this programme, a comprehensive RoPA will have been produced, together with central repositories of related Information Governance documentation, such as Data Protection Impact Assessments, Data Sharing Agreements, Data Processing Agreements, Privacy Notices, service delivery contracts.
- 3.4 Subject Access Requests (SAR) and Freedom of Information (FOI) Requests
- 3.4.1 Since its establishment in April 2022, the Business Support service has proactively and rigorously pursued the completion of all SAR and FOI requests.
- 3.4.2 As a result, the backlogs of SARs and FOIs has reduced significantly.
- 3.4.3 By mid November 2022, there were 36 SARs not replied to and out of timescales for response, about half of the number at the start of the financial year. Of these, 31 related to Childrens Services requests and 5 related to all other Council departments. This is due to the highly detailed, complex, and sensitive data involved with a Childrens' response. There are a further 13 SARs within timescales, 11 of which relate to Childrens.
- 3.4.4 Even better progress has been achieved against FOI responses. In the last report to Audit Committee, it was reported that at the end of May 2022, there were 60 FOIs beyond their response time, a significant reduction since the start of the year. By mid-November, this figure stood at 8. The length of delay ranges from 1 day to 225 days, with the average delay being 39.5 days.
- 3.4.5 FOI response times have also improved. In May, responses in timescale were reported as 56%, whereas in October, this figure was 100%.
- 3.4.6 These improvements are testimony to the effectiveness of the way Business Support has managed the SAR and FOI processes.

3.5 Data Breaches

- 3.5.1 As mentioned in previous reports, data breach monitoring continues to remain a high priority for the Council. Advisory letters continue to be sent by the DPO to officers responsible for a breach and Executive Directors and the DPO meet with them to identify learning and support needs.
- 3.5.2 There have also been additional briefings by the DPO and action plans developed by service managers where services have reported a number of data breaches. This has had a positive effect on performance and awareness with a reduction of further data breaches.
- 3.5.3 The majority of breaches continue to relate to data being sent to incorrect recipients.
- 3.5.3 All breaches reported are shown in the table below, which has been updated since the last report to Audit Committee.

3.5.4 For the period March 2022 to October 2022, the following breaches have been recorded by department:

	BGI	CC	CC-Finance	CYP	OCO	Ops	TOTAL	COMMENTS
March	0	5	0	2	4	1	12	Eleven involved information sent to wrong recipients. One involved information being shared inappropriately. Two reported to ICO both now closed
April	0	3	0	2	2	0	6	All involved information shared with wrong recipients.
May	1	7	0	4	6	1	19	Thirteen involved information sent to wrong recipient. Three involved information left unattended. Two involved information being inappropriately shared. One reported to the ICO. ICO decision pending until further information received from the Council.
June	0	3	0	3	1	0	7	Five breaches sent to wrong recipient. One involved data being sent to own personal email. One involved information left unattended.
July	0	5	0	1	1	0	7	All due to being sent to wrong addressee.
August	0	3	4	0	3	1	11	Nine related to wrong addressee. One related to accessing of information without permission. One related to information being stored in wrong place.
September	1	3	0	1	1	0	6	Four related to wrong addressee. One sharing information without consent/misunderstanding. One due to lost badge.
October	0	1	0	1	1	0	3	All due to being sent to wrong addressee.

3.6 Elected Member Support

- 3.6.1 Following the training offered to and attended by 21 Councillors earlier this year, further training is planned for the coming year.
- 3.6.2 All members have been given access to online training. By mid-November, 16 Councillors have completed the training, representing 31.4%, an increase from the 21.6% reported as completing by the end of June 2022.

4.0 Recommendations and Next Steps

- 4.1 The Audit Committee is required to note the 2022/23 performance to the end of November 2022.

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 UK General Data Protection Regulations (GDPR) 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:

This report provides an update to audit committee regarding the embedding of our obligations across the organisation. 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.

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:

Report to Audit Committee - Information Governance – ICO Update & Q2 delivery Update – 30 September 2021

Report to Audit Committee – Information Governance – Update Q3, 2021/22 to date – 25 November 2021

Report to Audit Committee – Information Governance – Update Q4, 2021/22 to date – 15 March 2022

Report to Audit Committee – Information Governance Update – 25 July 2022

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

Term	Meaning
BGI	Business Growth and Investment
CC	Corporate Core
CC-Finance	Corporate Core Finance
CYP	Children and Young People
DFM	Data Flow Mapping
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSPT	Data Security and Protection Toolkit
EIR	Environmental Information Regulations
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
IGSG	Information Governance Steering Group
OCO	One Commissioning Organisation
Ops	Operations
NHS	National Health Service
ROPA	Record of Processing activity
SAR	Subject Access Request
SIRO	Senior Information Risk Officer