Classification Open	Item No.

Meeting:	Audit Committee
Meeting date:	12th October 2023
Title of report:	Information Governance Update
Report by:	Julie Gallagher, Democratic Services Manager and Data Protection Officer
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. 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 reducing the levels of training non-compliance, and reinforcing lessons learned from data breaches.

Recommendation(s)

That Audit Committee note the 2023/24 performance from May to 30 September 2023.

Key considerations

Background

This report is to update Audit Committee on the Council's Information Governance activity up to the end of September 2023. As mentioned in the report to the July 2022 committee meeting, these reports now focus on the Council's 'business as usual' performance in the delivery of Information Governance.

Update of the Record of Processing Activities (RoPA)

Extensive work has previously been carried out to update the RoPA since the time of the ICO's visit in 2021 in order to develop a comprehensive RoPA, 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.

Since the staffing changes in May, however, the Information Governance team does not have capacity to develop the RoPA and as such no progress has been made since that time. Recruitment for a new IG Manager is ongoing, at which time work to continue the RoPA will recommence.

Subject Access Requests (SAR) and SAR reviews

From May to 30 September 2023 we received 92 SARs

May: 19 SARs across the Council

June: 19 SARs across the Council

July: 18 SARs across the Council

August: 17 SARs across the Council

September: 19 SARs across the Council

We are currently developing a new approach to logging requests for SAR reviews, but we have received approximately nine reviews for Children's Services SARs.

We have experienced issues with delays in responding to SARs from the Children and Young People Directorate. When the requestor is unhappy with either the outcome of the SAR or the timescales involved the DPO undertakes a review of how the request was handled. The delays and issues have led to a number of DPO reviews and, in addition, investigations from the ICO regarding timescales.

These delays are a result of a number of factors: officers and social workers were replying to a number of similar SAR requests at the time, and there was a fairly large amount of information being collated.

When we receive a SAR the Business Support team undertake a thorough sift of the information before it is referred to a social work team manager for them to undertake further sifts and checks. As a result of the issues outlined above, in a particular case there was a delay in a social worker making time to check all the information sent out to ensure that any third party information was redacted, and this resulted in a data breach. The delays in this particular incident were as a result of the social worker's availability to undertake this second sift of the information.

These problems have been raised and discussed with Senior Managers in both Children's Services and Business Support to avoid this recurring in future. Both service areas are looking into changing procedures and processes to do this, including the recruitment of additional social work staff.

Freedom of Information (FOI) Requests and Reviews

From May to 30 September 2023 we received 179 FOIs

From May to 30 September 2023 we received 7 requests to review FOI responses.

	May	June	July	Aug	Sep
Total FOI Requests received	33	38	31	44	33
FOI Reviews	2	0	1	1	3

It should be noted that a significant number of FOI reviews were left outstanding following the previous IG Manager's departure and officers have been working to close these cases. These historical reviews are being closed, but with severely delayed timescales. Members are assured, however, that these delays will not continue for future reviews now this backlog of FOI reviews has been addressed and a new casework management tool for FOI is being introduced as a result of a review of our systems and processes relating to the management of Freedom of Information requests.

The system changes will improve our case management and reporting arrangements, so that performance reporting is more efficient as we will minimise the time spent on the manual intervention, which will release capacity for quality checking. It will also provide additional benefits of increased automation, for example requestors will receive an automatic acknowledgement; reminders will be issued at key stages leading up to the 20 working day deadline to mitigate delays, and strengthened record keeping which will also be automated.

Data Breaches

From May to 30 September 2023 we received a total of 56 breaches.

	May	June	July	August	September
BGI	0	3	1	0	0
Corp. Core	3	4	6	9	3
CYP	2	2	3	2	5
Health & Adult Care	2	3	1	1	1
Operations	1	0	2	1	1
Other	1	0	0	0	0
Total	**9**	**12**	**13**	**13**	**10**

Although numbers have seen an increase, this is continuing a trend observed from the last 12 months following promotion of awareness of the need to report data breaches.

Officers are therefore confident that these figures reflect the better reporting practices, rather than mistakes happening more. This is supported by the large number of emails and calls IG officers receive asking for general IG advice (i.e. determining whether a breach has occurred, asking for guidance before sending responses, enquiring about good practice, etc.).

Members are assured that the vast majority of these breaches are relatively minor mistakes, with limited risk of harm to individuals. Almost all breaches are due to human error. Some of the themes and recurring issues are that of:

- Incorrect contact information being used (either from auto-populated addresses or similarly named recipients);
- Incorrect information on service software;
- Attachments not being double checked before being sent.

The DPO reviews every data breach and provides advice in terms of mitigation (e.g. further training, implementing an auto-delay on emails being sent, informing those affected etc.) to close off risk of harm to the individuals involved, and to learn lessons from the mistake and prevent it happening again. We log all data breaches; these are shared with the Exec team and the Corporate Governance Group, and a letter is sent to the person undertaking the breach.

For more serious breaches (generally those that involve children or vulnerable people's data), the DPO contacts the ICO for advice and assistance. For example, the incorrectly redacted SAR case outlined above was proactively reported to the ICO which was deemed no further action upon their review.

Complaints upheld by the ICO

From May to end of September 2023, we received no decision notices from the ICO. We are awaiting the ICO's response on one outstanding case currently.

Despite no decision notices being issued, the ICO have issued warnings over delayed timescales. These are predominantly the Children's Services responses to SARs, as outlined previously in this report.

The DPO has a good working relationship with ICO, contacting them as needed for advice and guidance on more serious breaches. Most of these are not reportable, and ICO officers are satisfied with the actions Bury Council has taken as a result of breaches which indicates our response and mitigation actions are appropriate, proportionate, and prompt.

Training

Training is monitored on a monthly basis, with a spreadsheet of non-compliant officers considered by IG Officers, the Exec Team, and the Corporate Governance Group. The DPO sends through a spreadsheet of non-compliant officers with Executive Directors and Assistant Directors, who then share names with relevant Heads of Service, who should

then liaise with officers (either directly or through Line Managers) to highlight the importance of completing this training in the next two weeks.

If, two weeks later, any officers still appear on the list of non-compliance, the DPO will send a warning directly to officers to let the officer know their access to ICT will be revoked should the training not be carried out within a two week period. If this is missed again, access will be revoked.

This process has been underway since July; the non-compliance figures for each department are as follows:

	July	August	September	October
BGI (111 staff in department)	11 users (recurrent not tracked)	12 users ↑ 7 recurrent	15 users ↑ 10 recurrent ↑	6 users ↓ 4 recurrent ↓
Corporate Core (373 staff in department)	23 users (recurrent not tracked)	33 users ↑ 15 recurrent	29 users ↓ 21 recurrent ↑	15 users ↓ 8 recurrent ↓
CYP (512 staff in department)	82 users (recurrent not tracked)	87 users ↑ 74 recurrent	135 users ↑ 71 recurrent ↓	114 users ↓ 106 recurrent ↑
Finance (152 staff in department)	21 users (recurrent not tracked)	17 users ↓ 12 recurrent	17 users ⇔ 11 recurrent ↓	4 users ↓ 3 recurrent ↓
Health & Adult Care (431 staff in department)	68 users (recurrent not tracked)	57 users ↓ 43 recurrent	62 users ↑ 46 recurrent ↑	48 users ↓ 39 recurrent ↓
Operations (866 staff in department)	265 users (recurrent not tracked)	262 users ↓ 252 recurrent	275 users ↑ 248 recurrent ↓	294 users ↑ 271 recurrent ↑

Non-compliance broadly increased from August to September, likely as a result of summer holidays and annual leave. Figures then mostly reduced in October, probably due to officers returning in September from leave and catching up with training requirements.

It should be noted that Ops have high numbers of non-compliance, but this is skewed from the large number of frontline staff who do not have regular access to ICT and are unable to complete the training online. The current process for frontline staff is that they are talked through a hard copy training guide as part of a 'toolbox talk' or team meeting. Once complete, the manager completes a spreadsheet and sends it to PSD to update training records, but this can take some time to process and feed into the figures IG officers receive. Although holding the highest levels of non-compliance, it should be noted that Operations teams are responsible for very few data breaches, reflecting the high number of frontline staff who do not habitually interact with personal data.

Compliance remains an area that officers are working to improve, with Exec Team regularly informed of non-compliance figures.

Community impact/links with Community Strategy

Equality Impact and considerations:

Equality Analysis	*Please provide a written explanation of the outcome(s) of either conducting an initial or full EA.*
N/A	

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:

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:
Julie Gallagher
Democratic Services Manager and Data Protection Officer
julie.gallagher@bury.gov.uk

Background papers:

Report to Audit Committee 1 December 2022 - https://councildecisions.bury.gov.uk/documents/s33397/Information%20Governance%20Update%20011222%20Final.pdf

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

Term	Meaning
BGI	Business Growth and Improvement
CYP	Children and Young People
DPO	Data Protection Officer
FOIA	Freedom of Information Act 2000
GDPR	General Data Protection Regulations 2018
HAC	Health and Adult Care
IG	Information Governance
Ops	Operations

ROPA	Record of Processing activity
SAR	Subject Access Request