

Classification	Item No.
Open	

<b>Meeting:</b>	Audit Committee
<b>Meeting date:</b>	6 <sup>th</sup> March 2024
<b>Title of report:</b>	Information Governance Update
<b>Report by:</b>	Julie Gallagher, Democratic Services Manager and Data Protection Officer
<b>Decision Type:</b>	For Information
<b>Ward(s) to which report relates</b>	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.

### Recommendation(s)

That Audit Committee note the performance from 1 October 2023 to 31 January 2024.

### Key considerations

#### Background

This report is to update Audit Committee on the Council's Information Governance activity up to the end of January 2024. 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.

### Proposed Changes to the Business and Executive Support Service, including Information Governance Responsibilities

The Business and Executive Support Service went live in April 2022. Since then, the ambition of reducing the administrative workforce by c20% to deliver financial savings has been achieved, together with a reduced reliance on agency staff. In total the Service has delivered £1.13m in savings. Several improvements have been made to ensure that business support processes are more efficient and effective, with inherited backlogs in April 2022 being managed and an increased focus on performance and delivery.

Although feedback suggests the ambition of business support being a flexible resource, moving staff to meet priorities. One area where the corporate team has proved particularly effective is in addressing policy compliance issues, in particular in relation to FOIs and SARs. Therefore, in evolving the service model, consideration has been given to how capacity can be maintained to focus on this area and expand this team's remit to include formal complaints, Members' Casework and MP enquiries, which represent three areas where additional capacity is needed based on current issues in relation to compliance and quality.

Three posts outside of the current function have also been considered as part of these proposals: the vacant Information Governance Manager role and the two posts currently focused on complaints management in the Customer Services function. In strengthening capacity in this area there is also an opportunity to connect this work to the activity and capabilities already in place within the Council's Democratic Services function.

In support of this aim, the service is also proposed to transition from the leadership of the Director of People & Inclusion to the Head of Democratic Services within the Law & Democracy Division of the Corporate core. This will bring together all Council functions which support policy compliance and democratic accountability and processes into a single area and, in particular, strengthen capacity and resilience in relation to Information Governance.

A new Policy Compliance Manager role evaluated at G13 will lead this team; it is this post that will strategic and operational responsibility for Information Governance matters, supported by the wider team.

Consultation has now closed and the finalised proposals will shortly be shared, it is a priority that vacant roles are recruited to.

### **Subject Access Requests (SAR) and SAR reviews**

From October 2023 to the end of January 2024 we received 80 SARs (across the Council).

- 1st October – 1st November 2023: 14 SARs
- 1st November – 1st December 2023: 23 SARs
- 1st December – 31st January 2024: 43 SARs

We also received approximately 4 requests for SAR reviews (this number can be misleading, as SAR requestors often respond with formal complaints rather than SAR review requests).

With regards to the delays previously reported to the Committee, timescales regarding final checks of SAR responses have improved, however a backlog is expected in the coming months owing to high volume of requests (at time of writing, 17 SARs have been received for Children's Services since the end of January) and staffing pressures unable to meet this demand.

The restructure and staffing changes outlined earlier in this report will help address these kinds of problems in the future, enabling a flexible response in terms of Policy Compliance staff available to process SARs. Ongoing staffing pressures in Children’s Services and the subsequent impact on SAR responses (which can take a lot of time to sift through information and redact appropriately) is an area IG and the new Policy Compliance Team are mindful of and will be an area of focus moving forwards.

**Freedom of Information (FOI) Requests and Reviews**

From October 2023 to January 2024 we received 452 FOIs

From October 2023 to January 2024 we received 4 requests to review FOI responses.

	Oct	Nov	Dec	Jan
Total FOI Requests received	107	111	89	145
FOI Reviews	1	2	0	1

Officers in the Business Support Team have been working on a new system to process FOI requests using Caseviewer, which is currently used for Members’ casework. This new system aims to streamline and remove duplication, improve reporting, and strengthen quality assurance, with FOI Lead sign off built into the system.

Statutory deadlines won’t change, with each FOI having 20 working days for completion (‘day 1’ is first working day after the request has been received). FOIs will be allocated by Service Area, containing several Champions & Leads, and automated notification emails and reminders will be sent to all staff within this Service Area, informing them a new FOI has been allocated.

The Service Area Champion is then responsible for reviewing the FOI, collating the relevant information and drafting a response. If necessary, Exemption & Extension Requests will go directly to IG officers for consideration before going back to the Champion to complete the draft response. This is then uploaded to the system for sign-off by the relevant Lead, after which the final response will be sent to the requestor by the Policy Compliance officers.

The Business Support Team (now becoming the Policy Compliance Team) will be running training sessions for all FOI Champions and Leads on the new system from March.

**Data Breaches**

From October 2023 to January 2024 we received a total of 35 breaches.

	October	November	December	January
BGI	1	1	0	0

Corp. Core	5	2	2	8
CYP	1	0	2	2
Health & Adult Care	1	2	1	3
Operations	1	4	0	0
<b>Total</b>	<b>9</b>	<b>9</b>	<b>5</b>	<b>13</b>

These numbers are consistent with the trend we have observed since the last 12 months. December had an uncharacteristically low number of breaches (most likely from the large proportion of staff leave during the month) but January saw a slight rise in breaches (most of which from the Corporate Core Directorate).

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. The most common themes and recurring issues are the same as in previous months, being:

- 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 Executive 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. We have had none such cases during the four-month reporting period.

### **Complaints upheld by the ICO**

We have had no complaints upheld by the ICO, and no issues reportable to the ICO.

### **Training**

Current training non-compliance figures are set out below:

<b>BGI</b>	<b>Corporate Core</b>	<b>Children's Services</b>	<b>Finance</b>	<b>Health &amp; Adult Care</b>	<b>Operations</b>
------------	-----------------------	----------------------------	----------------	--------------------------------	-------------------

(111 staff in department)	(373 staff in department)	(512 staff in department)	(152 staff in department)	(431 staff in department)	(866 staff in department)
1 officer non-compliant (0.9%) *	14 officers non-compliant (3.75%) *	46 officers non-compliant (8.98%)	0 officers non-compliant (0%)	23 officers non-compliant (5.34%)	108 officers non-compliant (12.47%)

A spreadsheet of non-compliant officers is regularly considered by IG Officers, the Exec Team, and the Corporate Governance Group. The officers' names are highlighted to Executive Directors and Assistant Directors to ensure training is completed in the following two weeks where possible, and reasons why are fed back when not.

It was originally planned that if any officers remained non-compliant after subsequent warnings, their access to ICT would be revoked. ICT have advised they are unable to carry this out. Officers continue to work with ICT to establish how this could be achieved.

It should be noted that Ops have high numbers of non-compliance but, as noted in previous reports, 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. Instead, these staff are talked through a hard copy training guide and training records are manually updated. These talks cannot take place 'ad hoc' like other staff able to complete online training so figures will generally be higher.

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.

---

**Equality Impact and considerations:**

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

---

**Assessment of Risk:**

The following risks apply to the decision:

<b>Risk / opportunity</b>	<b>Mitigation</b>
---------------------------	-------------------

<p>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.</p>	<p>Approval and Implementation of the Information Governance Framework.</p> <p>Implementation of a comprehensive Information Governance work programme.</p>
--	---

**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](mailto:julie.gallagher@bury.gov.uk)

**Background papers:**

Report to Audit Committee 12 October 2023 -  
<https://councildecisions.bury.gov.uk/documents/s37322/IG%20Report%20to%20Audit%20Committee%20Oct%202023.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