

SUBJECT:	INFORMATION GOVERNANCE UPDATE
DIRECTORATE:	CHIEF EXECUTIVE AND TOWN CLERK
REPORT AUTHOR:	DATA PROTECTION OFFICER (DPO)

1.1 Purpose of Report

To update Committee on the Council's Information Governance compliance and associated risks. This includes monitoring of compliance with the Data Protection Legislation including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA). This report also includes monitoring of the Council's compliance with its legal duties under the Freedom of Information Act 2000.

2. Background of Reporting

- 2.1 Reports are submitted on a six-monthly basis in line with reports submitted to Corporate Leadership Team. The last report provided to Committee was 12 December 2023.

3. Information Governance (IG) Risk Register

- 3.1 Attached at Appendix A (Part B) is the updated Information Governance Risk Register. The following risks are highlighted for comment as being risks where ongoing monitoring is required or further work is being carried out or is required.
- 3.2 There are currently no red risks on the Register. All Risks have an Assurance status of 'Substantial' and a direction of travel of 'Static' provided current control measures remain in place. This is with the exception of one risk which has an Assurance status of 'Limited' and a 'Declining' direction of travel (Risk 5) which relates to the retention and disposal of personal data.

4 Training (Risk 1)

- 4.1 Data protection training is a legal requirement. The Council renew training annually for all:
- staff
 - members
 - Information Asset Owners (IAO's) /service managers -receive a higher level of training.
 - New staff and members also receive training on induction.

Online training is accredited by the National Cyber Security Centre (NCSC) namely 'Cyber Ninjas' and covers both data protection and cyber security training. This year's course included new modules on ransomware, phishing, and email use. Service areas are also able to request additional face to face team training.

- 4.2 Members were offered face to face training on the 29 February 2024. Members who were unable to attend the face-to-face training were asked to complete the online bespoke member training offered by Cyber Ninjas.
- 4.3 Training compliance rates are good, and the small number of remaining non-completers are being chased through relevant managers and Assistant Director's.

Current completion rates are:

- All staff online training cyber ninjas (502 users completed, 21 in progress, 69 not started- 85% completion).
- low risk forms for those staff who do not normally process personal data. (41 responses).
- IAO higher level training for service managers. (35 completed, 1 in progress- 97% completion).
- Member training (13 completed, 18 not started- 42% completion).

However as explained to Committee previously the non-starters list includes staff on long term leave and staff who have recently left the Council and their accounts are yet to be deleted. This means the completion rate is likely to be much higher than 85% when taking these into account. Member training has also been delayed by the local elections although reminders have since been reissued and new members have received induction training.

- 4.5 The Council is considering deploying a simulated phishing exercise to all council network users including staff and members sometime this year. This is as a business continuity and training exercise, and which will also test the council's security measures. This is part of a programme of training relating to the risk of 'phishing' attacks which are the most common cause of cyber-attack, according to NCSC research. The Council's programme of training began with the Cyber Ninjas online training which includes guidance on how to identify a 'phishing' email. The programme of training continues with the current communications campaign 'Think before you click'.
- 4.6 All Information Asset Owners have completed their IAO Checklists for this year, and which are submitted annually. These checklists are self-declared mini audits of compliance in their own area with data protection. Any requests for assistance or queries have been or are being dealt with directly, including requests for additional team training. In summary there are no major areas of concern or non-compliance being reported by IAO's in their own service areas.

5. Data Protection Reform (Risk 3- Policies and Procedures)

- 5.1 The Data Protection and Digital Information Bill proposes reform to the existing Data Protection Legislation. The Bill is at Report Stage in the House of Lords with many amendments being tabled. The aim of the Bill is to cut paperwork for British businesses and enable personal data to be shared more easily, when in the public interest.

5.2 An update will be provided to Committee on how the Bill impacts the Council, if and when this becomes law. The Council's policies and procedures will also need to be reviewed and updated at this time. The Data Protection Officer will continue to monitor the Bills progress. The time limit for the Bill to be passed into Law has recently been extended by the government to December 2024.

5.3 The use of Artificial Intelligence (AI) by the Council is being considered including the risks, rewards, and the Council's readiness for this. Good governance and data quality is essential for AI to be used responsibly and a Policy is currently in development for internal acceptable use. There are huge potential benefits from the use of AI for the Council to harness including improved productivity, efficiency, and outcomes for customers. However, there are also high levels of risk such as bias within data, poor data quality, lack of transparency/explainability and digital exclusion to be considered.

6. Retention and Disposal of Personal Data (Risk 5)

6.1 It is essential that retention and disposal of personal data is automated as soon as possible in Office 365. Also, existing data held on premise is cleansed or deleted before migration to the Cloud. This ensures personal data is not retained longer than necessary which is key to business efficiency and transformation of the Council (including use of innovative technologies such as AI). There is extensive work to be completed by the Council in this area. This explains why the direction of travel for this risk on the IG Risk Register is 'Declining' and has a current Assurance level of 'Limited'. However, preliminary work on migration to the Cloud has begun, including review and retention or deletion of existing data as part of the IT migration project.

6.2 Currently IAO's/service managers declare retention and disposal is being implemented in their area, in their annual IAO Checklists and in accordance with their area's retention schedules. This is mainly a manual process although many of the Council's IT systems now automate these processes. It is critical that new IT systems procured by the Council have the capability for automated retention policies to be applied going forward.

7. Data Subject's Rights (Risk 8)

7.1 The Council continue to manage data protection requests from individuals regarding their own personal data (Subject Access Requests). Also, third-party requests for personal data, such as from the police, legal representatives, and insurance companies. These requests can be resource intensive often involving high volumes of data. The legal time limit for the Council to respond is 1 calendar month although this can be extended up to 3 months in certain circumstances.

7.2 By way of example, for the quarter Oct-Dec 2023 the council received 18 requests and 94% were responded to in time. A new e-form process for these types of requests went live on the Council's website in December 2023. This has made the process more accessible for requesters and easier for the Council to track, monitor and report. However, requests continue to be made using multiple channels including email, verbal, via complaints and claims. The council can only encourage requesters to use the online form.

8 Freedom of Information Requests

- 8.1 The Council receives Freedom of Information (FOI) requests in high volumes and Environmental Information Regulations (EIR) requests. For FOI requests the legal time limit for the Council to respond is 20 working days. This is a short time scale when requests can often involve large amounts of council held information.
- 8.2 By way of example, the council received 206 requests in the same period Oct-Dec 2023 and 87% were responded to in time. This is in addition to the data protection requests detailed above. In January 2024 the completion rate was 90% for FOI requests and any delays tend to be between 1-5 working days only and the Council have no requests outstanding more than 3 months from their deadline.
- 8.3 FOI response rates continue to improve following several actions including additional training for relevant officers, reducing the internal time scale for providing data and copying Assistant Directors into delayed responses from service areas. Further improvements are also planned to the current FOI e-form system available on the Council's website. FOI performance rates are to be published on the council's website on a quarterly basis from June 2024.

9. Annual Governance Statement (AGS)

- 9.1 The AGS status for Information Governance was downgraded from Red to Amber due to progress made previously following the implementation of the GDPR now UK GDPR. IG has since been removed from the AGS although remains closely monitored with reports being submitted biannually to IG Board (Corporate Leadership Team), and Audit Committee. Also reports to Corporate Management Team on specific IG issues as when required.

10. Strategic Priorities

- 10.1 This work ensures that staff and members are high performing in their collection and processing of customer and staff personal data. It also assists to ensure that the Council is 'trusted to deliver' services and compliant with the Data Protection Legislation.

11. Organisational Impacts

- 11.1 Finance (including whole life costs where applicable)

There are no financial implications arising from this report, as the resources will come from existing budgets.

- 11.2 Legal Implications including Procurement Rules

There are no legal implications arising out of this report.

11.3 Equality, Diversity and Human Rights

The Public Sector Equality Duty means that the Council must consider all individuals when carrying out their day-to-day work, in shaping policy, delivering services and in relation to their own employees.

It requires that public bodies have due regard to the need to:

- Eliminate discrimination.
- Advance equality of opportunity
- Foster good relations between different people when carrying out their activities.

There is no impact arising from this report regarding these issues.

12. Risk Implications

- 12.1 The Council must comply with the Data Protection Legislation. Non-compliance may result in enforced external audits, enforcement notices, monetary fines, criminal prosecutions of individual's, compensation claims and loss of public/partner trust. Non-compliance with the Freedom of Information Act 2000 may result in loss of public trust and enforcement action.

13. Recommendation

- 13.1 To note the content of the report and IG Register and provide any comment.

Is this a key decision? No

Do the exempt information categories apply? No

Does Rule 15 of the Scrutiny Procedure Rules (call-in and urgency) apply? No

How many appendices does the report contain? 1

List of Background Papers: None

Lead Officer: Sally Brooks, Data Protection Officer,
Email: sally.brooks@lincoln.gov.uk