AUDIT COMMITTEE **10 DECEMBER 2024**

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

1. Purpose of Report

1.1. To update Committee on the Council's Information Governance compliance and associated risks.

1.2. This includes compliance with the Data Protection Legislation including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA).

1.3. This report also includes monitoring of the Council's compliance with its legal obligations under the Freedom of Information Act 2000.

2. Background of Reporting

2.1. Reports are submitted biannually to Committee and in line with reports submitted to Corporate Leadership Team (IG Board). The last report provided to Committee was 4 June 2024.

3. Information Governance (IG) risk register

3.1 Attached at Appendix A (Part B) is the updated Information Governance Risk Register. There are currently no red risks detailed on the register and one risk (risk 5) with declining Assurance.

3.2 All risks detailed on the register require continuous actions and monitoring to ensure current Assurance levels are maintained.

3.3 The following risks are highlighted for comment in this report:

- training,
- policies, and procedures (proposed legislation changes),
- retention and disposal of personal data,
- data subject's rights and freedom of information requests.

4 Training (risk 1)

4.1 Data protection training is a legal requirement, and the Council renew training annually for the following:

- low risk staff-receive a basic level of training
- general staff
- elected members

- Information Asset Owners (IAO's) (Service Managers) -receive a higher level of training.

4.2 New staff and members also receive training on induction.

4.3 The Council's current training 'Cyber Ninjas' is accredited by the National Cyber Security Centre (NCSC) and covers data protection and cyber security training. The Council have recently obtained a 'refresh' of the training package due to be deployed in early 2025.

4.4 Training compliance rates are good, currently 91% for general staff. The small number of remaining non-completers are being chased through relevant Service Managers and Assistant Directors.

4.5 If the Council is required to report a serious data breach to the regulator the Information Commissioner's Office (ICO), it must confirm the staff or member involved has received data protection training in last 2 years. If this cannot be confirmed the Council may be subject to enforcement action.

4.6 The Council currently has a comms campaign 'Think before you click'. This includes regular news, posts, video clips and posters displayed around Council offices. These provide staff and members with everyday tips to protect data such as how to identify phishing emails and to reduce the risk of data breaches.

5. Policies and Procedures (risk 3) proposed legislation changes

5.1 The former 'Data Protection and Digital Information Bill' (DPDI) which proposed reform of the Data Protection Legislation was dropped following the calling of the General Election in May 2024.

5.2 The Data (Use and Access) Bill (DUAB) was introduced on 23 October 2024. The bill contains many provisions from the DPDI and proposes amendments to the DPA 2018 and UK GDPR. Some of the provisions from the DPDI have not remained and other new provisions have been added.

5.3 Please see House of Lords briefing note for further information on the bill Data (Use and Access) Bill [HL]. The Council will need to monitor the progress of the bill and amend its data protection policies and procedures to reflect any changes in legislation.

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

6.1 Deletion of personal data beyond its retention period is a legal requirement. The Council has reduced personal data held in physical form (such as paper records) in recent years and now needs to continue to concentrate on its electronic data.

6.2 Electronic data held by the Council needs to be analysed, reviewed and deleted where required. In particular before data is migrated to the Cloud. This is key to business efficiency and transformation. This also limits the impact on individuals and the Council in relation to the amount of personal data included in data breaches and cyber-attacks.

6.3 IAOs declare retention is being implemented in their areas, in accordance with the Council's retention schedules. This is mainly a manual process, resource intensive and difficult to prioritise. This has resulted in an ongoing decline in Assurance, as more data is retained over time. Increasingly IT systems can automate retention. It is therefore critical retention capability is considered on procurement of new systems and implemented where possible in existing systems.

6.4 A detailed analysis of the electronic data the Council holds in each service area has begun as part of the IT migration project. This has commenced with an analysis of data held over 6 years which is being provided to IAO's for review and deletion. Work has also been carried out reviewing and deleting electronic data held in corporate wide drives.

6.5 The Council have agreed Microsoft Teams 1-1 Chats will have an automated short retention period. This function has been used by staff as a form of office chat and collaboration following the increase in remote working. Chat regarding customers and partners should be contained in Teams Channels as opposed to 1-1 Chat and therefore this will not be affected.

6.6 A retention period of 6 months has been agreed on 1-1 Chat with a 3 month lead up to implementation following this being communicated to staff and members. The 3 months lead up period will allow staff and members time for any data required to be retained, to be moved.

7. Data Subject's Rights (risk 8)

7.1 Completion rates for Data Protection Act requests (DPAs) are detailed below by quarter since last reported to Committee.

July-Sept 2024	
Total requests received	34
Requests completed in time	**97%**
April-June 2024	
Total requests received	35
Requests completed in time	**91%**

7.2 DPAs include Subject Access Requests (SARs) from individuals regarding their own personal data and also requests from third parties, requesting personal data such as the Police.

7.3 By way of comparison and detailed below see total DPA requests received and completion in time rates previously reported:

Time periods	**Total requests received**	**Percentage completed in time:**
Jan-March 2024	23	82%
Oct-Dec 2023	18	94%
July-Sept 2023	28	91%
April-June 2023	32	91%

Jan-March 2023	20	80%
Oct- Dec 2022	25	84%
July -Sept 2022	26	77%

7.4 The above tables (7.2 and 7.3) show completed in time rates have significantly improved over the last 2 years (increase of up to 20%) due to actions the Council have taken including changes in internal procedures for collating data from service areas.

7.5 An online form went live on the Council's website earlier this year for Subject Access Requests. In August this was made more prominent on the Council's 'Apply for it' web page. This has improved accessibility for requesters and the Council's ability to track, respond and report these requests more easily.

8. Freedom of Information Requests

8.1 Response rates for requests under the Freedom of Information Act 2000 (FOI) are detailed below by quarter since last reported to Committee.

July-Sept 2024	
Total requests received:	115
Requests completed in time:	**83%**
April-June 2024	
Total requests received:	181
Requests completed in time:	**86%**

8.2 By way of comparison, detailed below see total FOI requests received and completion in time rates previously reported:

Time periods	**Total requests received**	**Percentage completed in time:**
Jan-March 2024	179	85%
Oct-Dec 2023	206	87%
July-Sept 2023	200	89%
April-June 2023	174	86%
Jan-March 2023	205	89%
Oct- Dec 2022	95	61%
July -Sept 2022	75	54%

8.3 The above tables (8.1 and 8.2) show response rates have significantly improved over the last 2 years (increase of up to 35%) This is due to actions taken by the Council such as officer training. This improvement is despite the number of FOI requests significantly increasing over the last two years and remaining high.

8.4 Further improvements are still required to be considered 'good' by the ICO (95% or more). The aim is improvements will be made from an increased number of trained officers and a planned review of FOI internal processes.

8.5 FOI response rates are now published on the Council's website key FOI statistics to improve transparency and in line with guidance.

9. Annual Governance Statement (AGS)

9.1 Information Governance was removed from the AGS but remains closely monitored with reports biannually to IG Board (Corporate Leadership Team), and Audit Committee. It is also monitored by an internal working group incorporating the Senior Information Risk Officer, Data Protection Officer, Audit, Legal, IT Managers and Communications.

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 including the IG register (Appendix A) 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