AUDIT COMMITTEE **12 DECEMBER 2023**

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 Risk Assurance Levels. This includes monitoring the Council's compliance with the Data Protection Legislation including the UK General Data Protection Regulation, the Data Protection Act 2018, and the Freedom of Information Act 2000.

2. Background of Reporting

2.1. Reports are submitted every six months and the last report provided to Committee was on 6 June 2023.

3. Information Governance 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' when current controls 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) relating to the retention and disposal of personal data.

4 Data Protection Training (Risk 1)

4.1 Data protection training for all staff and members is a legal requirement. The Information Commissioner's Office (the UK regulator) recommends training is renewed every two years and preferably annually for an organisation such as the Council. The Council renew training annually and provide training on induction for staff and members.

4.2 The Council deploy online training accredited by the National Cyber Security Centre which covers both data protection and cyber security training. The need for cyber security training is essential given the increase in remote working for staff and cyber activity globally.

4.3 The training includes a higher-level package for Information Asset Owners (IAOs) being service managers 'Data Confident' and a bespoke package for members, 'Cyber Ninja's for Councillors'. Members have also been offered face to face training to go through this package scheduled on 29 February next year delivered by the Data Protection Officer and the Business Development and IT Manager.

4.4 The highest completion statistics for 2022 staff training were 85%. A report indicating 100% is not achievable as the staff list is constantly changing and as staff leave and new staff join the percentage rate will go down until the training is completed. There are also staff unable to carry out the training due to long term leave and those that remain on the staff list for a period of time after leaving the authority for various reasons. The

overall completion rate for 2022 is therefore higher than the report indicates, and this could be evidenced if required to the ICO.

4.5 Training is to be refreshed by all staff at the end of this year and will be issued in December 2023 to be completed by the end of January 2024. The training includes new modules on 'Ransomware' and 'Phishing email' cyber-attacks which are becoming increasingly common and more sophisticated. The staff list has been cleansed prior to deployment in an attempt to achieve a higher and more accurate completion rate. Completion by staff over the Christmas and New Year period has worked well in previous years. This will be promoted through staff communications with non-completers being followed up and reported to senior management.

4.6 IAO's are also currently refreshing their online training and have been asked to complete the new version of the higher-level training package by the end of December 2023. Non-completers will be followed up and reported to senior management.

4.7 IAO's completed their annual IAO checklists at the end of November 2023. This requires them to assess their information assets and compliance in their areas. This includes reviewing their section of the Council's Information Asset Register, Information Sharing Agreements register, Privacy notices and Contracts in their area. The outcome of these compliance checks will then be reported to the Senior Information Risk Officer and Corporate Leadership Team. IAOs were given the opportunity to request further data training for their teams and these sessions, where requested, will be carried out early next year.

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

5.1 Data Protection Reform is still being considered by Parliament in the Data Protection and Digital Information Bill (No.2). The Bill proposes amendments to the Data Protection Act 2018, UK GDPR and the Privacy and Electronic Communications Act. The Government states 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 The text of the Bill can be found here at Data Protection and Digital Information (No. 2) Bill - Parliamentary Bills - UK Parliament. The Bill is currently at Report stage in the House of Commons. The Council's relevant policies and procedures will need to be updated when and if this becomes Law.

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

6.1 It is essential that retention and disposal of personal data is implemented from the outset in Office 365 including Microsoft Teams and that existing data held on premise in electronic drives is cleansed or deleted as part of the migration to the Cloud. Retention and disposal should be applied on new data being created and being saved into the Office 365 suite. This will ensure the Council does not retain personal data longer than necessary. This is a fundamental principle of data protection compliance, key to business efficiency and reducing risk in relation to personal data breaches and information requests.

6.2 Suppliers were instructed to assist in migration and retention policies in Office 365 and have provided recommendations to the Council. Work on considering the Councils options for this is currently being undertaken by IT. An internal IG working group of key stakeholders including Legal, Data Protection Officer, Internal Audit, BDIT and the SIRO are advising and supporting the project along with specialist consultants where required. The use of Office 365 and Cloud for data storage by the Council is still however in its infancy and some way from standard retention periods. The Council want to ensure that migration to the Cloud and automated retention policies are implemented correctly and

in planned way, as not to disrupt service delivery. IAO's are responsible currently for ensuring retention policies are applied to any data held in their area.

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, from others such as the police, legal representatives, and insurance companies. These requests can be resource intensive often involving high volumes of data. There is a legal time limit for the Council to respond of 1 calendar month. By way of example, for the quarter April-June 2023 the council received '32' requests. A new e-form process for these types of requests is due to go live on the Council's website shortly. This will be more accessible for customers and will make it easier for the Council to track, monitor and report on requests.

8 Freedom of Information Requests

8.1 The Council continues to receive Freedom of Information (FOI) requests in high volumes. There is a legal time limit for the Council to respond of 20 working days. By way of example, the council received '174' requests in the same period April-June 2023 in addition to the data protection requests above. FOI response rates have been improved following several actions including training for relevant officers, reducing the internal time scale for proving data and copying Assistant Directors into delayed responses from service areas. Scheduled improvements are also planned to the current FOI e-form system.

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 as on specific 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's personal data. It also assists to ensure that the Council is trusted to deliver services and in compliance with the Data Protection Laws.

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.

13. Recommendation

13.1 To note the content of the report 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.brookes@lincoln.gov.uk