

**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 Information Governance. This includes monitoring of the council's compliance with data protection legislation including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA).

**2. Background of Reporting**

- 2.1. Reports are submitted on a bi-annual basis the last report being provided to committee in November 2022.

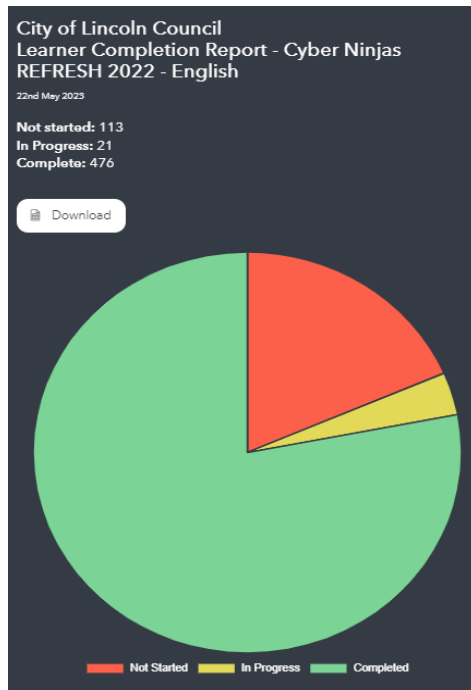
**3. Information Governance Risk Register**

- 3.1 Attached at Appendix A (Part B) is the updated Information Governance risk register. The following risks are highlighted for comment:

**4 Data Protection Training (Risk 1)**

- 4.1 Data protection training is a legal requirement. The Information Commissioner's Office (ICO UK regulator) recommends training is renewed every 2 years and preferably annually for an organisation such as the council. The council renew training annually for all staff/members and provide training for all staff/members on induction.
- 4.2 The council deploy training accredited by the National Cyber Security Centre (NCSC) which covers both data protection and cyber security training. The need for cyber security training is essential particularly given the increase in staff working remotely and cyber activity due to global events.
- 4.3 The training includes a higher-level package for Information Asset Owners (IAO's) all service managers and some team leaders) called 'Data Confident' and a bespoke training package for members, 'Cyber Ninja's for councillors' which reinforces members hold individual responsibility for data protection as 'controllers' when processing constituents' personal data.
- 4.4 As of 22 May 2023, the training completion level report indicates 85% completion by all staff and members for this year.

4.5



- 4.6 A report indicating 100% completion of training 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 those unable to carry out the training as on long term leave. Out of the 'Not started' report above approximately 69 have left the authority and 12 are on long term leave. The overall completion rate is therefore higher than the report indicates. The few remaining non-completers are now being followed up through their relevant Assistant Director as requested by the council's Senior Information Risk Officer (SIRO)
- 4.7 Staff without network access who do not normally process personal data as part of their role, complete a low-risk data protection form detailing the principles of data protection.
- 4.8 Training will need 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 as completion over this time period has worked well in previous years.
- 4.9 Members will also be offered face to face data protection training later this year by the Data Protection Officer.
- 4.10 IAO's complete an annual checklist which requires them to assess their information assets. This includes reviewing their section of the council's 'Information Asset Register' and ensuring information sharing agreements, privacy notices and contracts in their area are compliant. Also, to confirm personal data in their area is being confidentially disposed of in accordance with the council's retention and disposal schedules.

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

- 5.1 Data Protection Reform is currently being considered again by Parliament in the Data Protection and Digital Information Bill (No.2). This is after the previous version of the Bill was removed. The Bill proposes amendments to the Data

Protection Act 2018, UK GDPR and the Privacy and Electronic Communications Act. As with the previous Bill the Government states the aim is to cut paperwork for British businesses and enable personal data to be shared more easily particularly when in the public interest. 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 committee stage and the council's relevant policies/procedures will need to be updated when this becomes Law.

## **6. Retention And Disposal of Personal Data/Records (Risk 5)**

- 6.1 Office 365 has the potential to improve information management in terms of available tools on retention, sensitivity labelling, data leakage and access control as well as compliance and efficiency with information requests such as Freedom of Information and Data Protection Act (DPA) requests.
- 6.2 It is essential that retention and disposal of personal data is implemented from the outset in Office 365, and that existing data held in on premise electronic drives is cleansed and deleted where possible before any data is migrated. This will ensure the council does not retain personal data longer than necessary. This is a fundamental principle of data protection compliance and key to business efficiency. The council need to also ensure that retention and disposal policies are implemented from the outset 'privacy by design' on all new IT systems.
- 6.3 Suppliers were instructed to assist in migration and retention policies in Office 365 and have provided recommendations to the council. Work on piloting and implementing these recommendations in priority service areas is due to commence in August 2023 and now IT have successfully delivered the council's the new Telephony system.

## **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) and from third parties for personal data, such as the Police, legal representatives, and insurance companies. These requests can be resource intensive as they often involve complex legal issues and high volumes of data. There is also a time limit for the council to respond of 1 calendar month. By way of example, for the last full quarter Jan-March 2023 the council received '24' requests.
- 7.2 This is in addition to Freedom of Information (FOI) requests which the council continues to receive in high volumes. By way of example, the council received '216' requests in the same period Jan-March 2023 in addition to the data protection requests above.

## **8. Annual Governance Statement (Ags)**

- 8.1 The AGS status for Information Governance was downgraded from Red to Amber due to progress made in the implementation of the GDPR. IG has since been removed from the AGS although remains closely monitored with reports being submitted biannually to IG Board (CLT), and Audit Committee as well as CMT as and when required.

## **9. Strategic Priorities**

- 9.1 This work ensures that staff are high performing in their collection and processing of customer's data. It also assists to ensure that the council is trusted to deliver the services and ensures compliance.

## **10. Organisational Impacts**

- 10.1 Finance (including whole life costs where applicable)

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

- 10.2 Legal Implications including Procurement Rules

There are no legal implications arising out of this report.

- 10.3 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.

## **11. Risk Implications**

- 11.1 The council must comply with 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.

## **12. Recommendation**

- 12.1 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.brooks@lincoln.gov.uk](mailto:sally.brooks@lincoln.gov.uk)