ANNUAL REPORT OF THE SENIOR INFORMATION RISK OWNER 2024/25

1 Purpose of this report

1.1 This report provides a summary of Information Governance activity across Gedling Borough Council during 2024/25 in order to provide assurance that information risks are being managed effectively. The report also provides an update on the following:

- achievements for the period 1 April 2024 to 31 March 2025; the Council's compliance with legislative and regulatory requirements relating to the handling of information, including compliance with the General Data Protection Regulations 2016 (GDPR), Data Protection Act 2018 (DPA), Freedom of Information Act 2000 (FOI) and Environmental Information Regulations 2005 (EIR);
- data incidents relating to any loss or inappropriate access to personal data or breaches of confidentiality, and planned Information Governance activity during 2024/25.

2 Background

2.1 Information is a vital asset for the provision of services to the public and for the efficient management of the Council's resources. Without adequate levels of protection, confidentiality, integrity and availability of information, the Council will not be able to fulfil its obligations, including the provision of public services, or meet legal, statutory and contractual requirements.

2.2 There continues to be an increased threat of a cyber-attack, including the heightened posture recommend by the NCSC due to the war in Ukraine. An attack, if successful, will result in a significant impact on the Council's customers, staff and reputation. Most of the Council now relies on information technology on a day-to-day basis.

2.3 Information governance concerns the effective management of information in all its forms and locations, including electronic and paper records. It encompasses efficient ways of handling that information (how it is held, used and stored), robust management of the risks involved in the handling of information and compliance with regulatory and statutory guidance including the GDPR, DPA and FOI. Information governance is also concerned with keeping information safe and secure and ensuring it is appropriately shared when necessary to do so.

2.4 Senior Leadership approved an Information Security Governance Framework which was endorsed by Cabinet on 1 August 2019. The Deputy Chief Executive and Monitoring Officer is the designated Senior Information Risk Owner (SIRO). The SIRO is responsible for:

- Managing information risk in the Council.
- Chairing the Data Security Group (now incorporated into the Corporate Risk Board).
- Fostering a culture for protecting and using information within the Council.
- Ensuring information governance compliance with legislation and Council policies.
- For risk at SLT level, ensuring that risk is properly identified, managed and that appropriate assurance mechanisms exist.
- Preparing an annual information risk assessment for the Council.
- Giving strategic direction to the work of the Data Protection Officer (DPO).

2.5 The Council is required to appoint a DPO and this role is currently designated to the Legal Services Manager position. The DPO is assisted by a Deputy being the Legal Officer. A new Legal Services Manager was appointed in 2024/25 meaning there has been a change in DPO.

2.6 At the start of 2024/25 the Council had a Data Security Group (DSG) in place, the membership of which comprised the Deputy Chief Executive (Chair), Chief Finance Officer, Data Protection Officer or Deputy, and the Research and Development Manager (IT Support). During 2024/25 due to changes in corporate governance arrangements, a new Corporate Risk Board was established including the members above and all Assistant Directors across the Council. This board meets every other month, and data security now forms part of the agenda for this board with regular reporting by the DPO and Assistant Director for Digital, Data and Technology. The overarching remit of the group is to assist the Council to fulfil its obligations and monitor risk in respect of information governance and cyber security, to appropriately protect paper and electronic ‘data’ and to ensure that everyone who has authorised access to ‘data’ is aware of their ‘data handling’ responsibilities.

2.7 The Council has a set of high-level corporate policies in place which direct the Information Governance work. The key policies are:

- Information Security Policy.
- Data Protection Policy.
- Records Management Policy.
- Records Retention and Disposal Policy.
- Risk Management Strategy and Framework.

3 GDPR Information and Governance Internal Audit

3.1 In July 2024 the Council's internal auditors carried out an audit on the Council's data protection and information governance compliance. The audit focused on the following areas:

- *Assess whether there is a governance framework in place to support compliance with data protection responsibilities, including defined, approved and up to date policies and procedures.*
- *Determine whether roles and responsibilities with regards to data protection are defined and whether there is a training programme in place for data protection and information management for staff which is regularly refreshed.*
- *Assess whether the Council has a Record of Processing Activities in place and that this is regularly reviewed and updated and captures appropriate information.*
- *Assess whether the Council has defined retention periods in place for held information and that this is adhered to.*
- *Determine whether the Council has defined the lawful basis for collecting, processing, retaining, and sharing information and assess whether this is transparent to data subjects using tools such as privacy notices. For special category data, assess whether any additional reasons for processing are appropriate and in line with the original purpose of the processing activity.*
- *Assess whether there is regular monitoring of the Council's compliance with data protection legislation and regulations by senior management, including the identification, assessment, and remediation of risks.*
- *Assess whether there are procedures in place to deal with data subject rights requests, including Subject Access Requests (SARs), Freedom of Information Act requests (FOIs) and the exercising of rights by individuals. Determine the extent to which these requirements are complied with, responded to, monitored, and reported on.*
- *Assess whether adequate and effective data breach response procedures are in place.*
- *Assess whether there are adequate procedures in place for performing Data Protection Impact Assessments (DPIAs) for the processing of personal data which is likely to present a high risk to the rights and freedoms of individuals.*
- *Where the Council shares personal data as part of its relationships with third parties, determine whether the risks posed by these relationships have been assessed and whether data sharing agreements have been implemented to mitigate these risks.*

3.2 The audit found several good practices including:

- A dedicated DPO with clearly defined responsibilities.
- A dedicated team in place to manage compliance subject access and information requests.
- A defined Data Protection Policy which sets out the Council's approach towards compliance with the legislation.
- Privacy Policies in place and published on the Council's website which are regularly updated.
- A good understanding of data protection requirements across randomly selected service areas.
- A set process for reporting data breaches.
- Employees are required to complete mandatory data protection training.

3.3 The audit found three areas of improvement, one high and two low.

- High risk - Information Asset Register (IAR) not containing sufficient amounts of information with some service areas IAR's having a lot of blanks and no information.

- Low risk - Records Retention Policy was a low risk, the policy was last updated in 2020 and due a review.

- Low Risk – Data Protection Impact Assessments aren't covered in detail within the Data Protection Training.

3.4 Following the outcome of the audit an action plan to address the areas of improvement has been prepared and the actions put in place to address these areas are as follows;

- To replace IAR's with Records of Processing Activity (RoPA) containing more detail about the processing of personal data in each service area.
- To review and update the Records Retention Policy.
- To renew the Council's data protection training to include more focus on DPIA's and when they are needed.

4 Information Governance/Security Training carried out

4.1 Since the COVID pandemic the training programme for data protection has consisted of a virtual training programme accessible by all staff with computer access. The virtual training programme which consists of a video recorded training session followed by a short quiz was initially launched in December 2020. This remains the method of providing data protection training to Council Officers for 2024/25. However, following the outcome of the internal audit a new and updated training video and quiz has been produced. This new training provides more detailed focused on DPIA requirements as suggested by the audit findings and was rolled out across the Council at the beginning of 2025/26.

The DPO and Deputy provided a face-to-face session with Members following the local election in May 2023. This session was recorded and has been provided to Members along with the training slides for those who were unable to attend the face to face session. This recording remains available for Members should they wish to revisit the training at any time and for any new Members elected to the Council.

4.2 In addition to this where Departmental Representatives who are responsible for handling information requests have changed either due to restructure or staff departures, additional one to one training has been provided by the Deputy DPO via Microsoft Teams focusing on recognising and dealing with information requests and subject access requests and use of the Council's information request system.

4.3 Data Protection training is mandatory for all staff and forms part of the training checklist on induction. The virtual training package created by the DPO and deputy DPO is available on the Council's intranet and is accessible all year round for all staff including new starters. In terms of staff without IT access who do not process large amounts of personal data, training leaflets are provided.

4.4 The Council have continued to engage this year with the Nottinghamshire Information Officers' Group (NIOG) attending meetings which have been held on MS Teams. The group have assisted the Council in ensuring appropriate sharing agreements are in place using the NIOG template which is GDPR compliant. As part of the group Nottinghamshire County Council have created a MS Teams group and SharePoint site where all members of the group can access agendas and minutes of previous meetings and also share information and documentation.

4.5 A face-to-face briefing was given to Members on data security following the election in May 2023. Training materials for new starters and as refresher training for existing staff are however available on the Intranet and form part of the corporate mandatory training for all staff. An online cyber security training course (including a quiz) from the National Cyber Security Centre (NCSC) has now been made available to staff alongside the existing training material and this is continually promoted.

5 Requests for Information

5.1 The Council has an information request system for logging, monitoring and reporting on requests for information. The responsibility for managing information requests sits within Legal Services but every department within the Council has their own representative who can deal with requests for information on behalf of that department, provided the requests are straight forward and no exemptions or exceptions apply. Where a request is more complicated, exemptions/exceptions need to be applied, or it is a council wide request this is responded to by a member of the Legal Services team.

5.2 In 2024/25 the Council received 1020 requests for information made up of 118 EIR requests, 39 DPA subject access requests, 127 DPA exemption requests and 736 FOI requests. This is slight increase when compared to the number of requests received in 2023/24 (917).

5.3 In 2024/25 there were 6 requests to review a decision to withhold information, and no complaints were made to the Information Commissioner's Office (ICO).

6 Information Governance/Security Policy Review

6.1 The current Information Security Policy was originally approved by Cabinet on 4 April 2013 and has been subject to a number of amendments since then. A full review of the Information Security Policy was completed in 2022/23 amendments were brought forward for approval to Cabinet in 2023/24 as part of this annual reporting process. A further review of the policy is to be undertaken in 2025/26 along with the introduction of a new policy specifically linked to the use of Artificial intelligence.

6.2 The Data Protection Policy was updated and approved by SLT on 21 December 2022.

6.3 In order to improve security around the provision of information to customers and to standardise the approach across the Council a new Identification and verification Policy is being prepared. This will ensure a standardised approach to confirming the identity of customers prior to any personal information being disclosed.

7 Information/Security Incidents

7.1 In 2024/25, the Council has recorded 46 data breaches/incidents by council officers. Of the 46 reported breaches 39 were confirmed to be personal data breaches. No breaches were reported to the ICO as they were all minor in nature and did not meet the threshold for reporting.

7.2 The Council takes data breaches very seriously and has a robust reporting system in place to ensure compliance with the 72 hour reporting deadline. Reporting data breaches is something that is part of the corporate training programme but is also well publicised on the intranet, and through team meetings.

7.3 The breaches reported have been minor in nature and have largely been borne out of clerical error, for example reliance of autofill in outlook, the wrong addresses typed into systems which generates mail to the wrong address or multiple letters contained within one envelope. Staff have been reminded to check address details or update changes to addresses before sending out mail and to take care when posting external letters. Every incident is thoroughly investigated and wherever necessary, measures are put in place to reduce the risk of further incidents. To maintain corporate oversight, all incidents are reported to and considered by the DSG and now Corporate Risk Board. No systemic failures have been identified.

7.4 IT investigated 42 cyber security incidents last year. We are not aware of any successful Cyber Security Incidents involving Malware or Hacking in 2024/25.

7.5 62% of the security incidents involved phishing emails. This work is usually to inspect suspect emails, and sometimes to check for impacts of followed links. The Council continues to be subject to a large number of attempted phishing attacks which are stopped by a combination of technical controls and staff vigilance. Cyber security training delivered to members as part of their induction post-election and the online cyber security training available to staff and members has also raised awareness in relation to potential phishing attacks.

8 Summary of key achievements in 2024/25

8.1 The key achievements in 2024/25 are as follows:

- ICT officers continue to be active members of the East Midlands Government Warning, Advice and Reporting Point (EMGWARP).
- Achieved PSN CoCo compliance.
- Maintained Payment Card Industry Data Security Standard (PCI DSS) compliance.
- Mobile Device refresh completed
- Backup infrastructure refresh completed
- Continued Windows Server refresh
- Conducted IT Disaster Recovery Rehearsal and implemented recommended actions Commenced the annual review of existing Information Asset Registers and all Information Sharing Agreements.
- Completed administrative review of Information requests and updated departmental representatives accordingly.
- Increased engagement with the Business Design and Technology Authority to align procurement and system changes to enable better governance.
- We seek to ensure records are deleted when appropriate which is an ongoing task.
- Completed an internal audit on GDPR and Information Governance

compliance.

- GDPR mandatory training continues to be available to all staff. Updated data protection training has been prepared and ready to be rolled out in Q1 of 2025/26.
- Produced Record of Processing Activity to replace IAR's.
- Employed a new DPO.
- Employed a Temporary Information & Governance Support Officer to assist with information requests monitoring and compliance.
- Reduction in number of information requests with responses exceeding statutory deadlines.
- Established the Corporate Risk Board which is responsible for oversite of information security risks.

9 Plans for 2025/26

9.1 The following activity is planned for 2025/26:

- A review of Council's policies to ensure they remain fit for purpose, including: the Information Security Policy; and the Records and Retention Policy, for presentation to Cabinet for approval.
- Implement the Digital Data and Technology Strategy 2024-27.
- Create improved Identification and Verification procedures.
- Create a new Artificial Intelligence Policy.
- Continue to upgrade ICT infrastructure as required.
- Continue working on replacing legacy analogue telephone lines due to Public Switched Telephone Network switch off.
- Continue to work on national shutdown of 3G mobile network.
- React to any requirements from the Ministry of Housing Communities and Local Government (MHCLG) related to the Local Government Cyber Assessment Framework.
- Public Sector Network (PSN) compliance to be maintained.
- Maintain PCI DSS Compliance.
- Continue to develop the cyber security risk register.
- Upgrade SQL 2014 servers to newer version.
- Replace mobile devices to keep them in support.
- Conduct IT Disaster Recovery Rehearsal and implement recommended actions.
- Review networking arrangements.
- Start project to replace Windows 2016 Servers.
- Review Business Continuity Plans across the organisation to ensure they are fit for purpose in the event of a cyber security incident.
- Deliver additional DPIA training to identified officers.
- Review and update the Council's Records Retention policy.
- Continue to complete reviews of Data Protection Impact Assessments (DPIAs).
- Ensure continued compliance with GDPR in terms of breach reporting, DPIAs.
- Replace network switches in the Civic Centre.
- Refresh backup infrastructure with newer software and hardware.

10 Risk

10.1 It must be recognised that information governance and cyber-attacks are

significant risk areas for all organisations locally, nationally and globally. The risk of accidental data loss, physical system failures and direct malicious cyber- attacks are an ongoing concern for the Council requiring continuous focus.

10.2 The Council has a corporate Risk Management Strategy and Framework in place. A number of risks relating to Information Governance have been recorded on departmental risk registers and the new corporate risk register also includes two strategic risks of IT/Technology and Information data. Further development of the cyber risk register is planned for 2025/26.

11 Conclusion

11.1 The Council has a healthy culture of breach and incident reporting which needs to continue to ensure incidents are investigated, reporting requirements to the ICO are complied with and importantly, remedial action taken. Good progress has been made in improving information governance processes and maintaining GDPR compliance. The Council needs to continue with its robust and pro-active approach to the management of personal data.

11.2 The Council has robust cyber security arrangements in place and it is crucial that these are not only maintained but also continue to evolve to meet the cyber security challenges of today, and tomorrow. The incidents have demonstrated that robust security measures are in place to protect the council underpinned by robust processes and officer capability to deal with this type of unexpected event. However, the Council cannot stand still: continuous improvement needs to be made and cyber security must remain a priority. Changes to roles and responsibilities within the ICT team have enabled a more focused role dedicated to cyber security.