ANNUAL REPORT OF THE SENIOR INFORMATION RISK OWNER 2025/26

OFFICIAL – FOR PUBLIC RELEASE

1 Purpose of this report

1.1 This report provides a summary of Information Governance activity across Gedling Borough Council during 2025/26 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 2025 to 31 March 2026; 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 2025/26.

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.

2.6 At the start of 2025/26 the Council's information governance and data security arrangements continued to be overseen by the Corporate Risk Board. Membership of the Board comprises the Deputy Chief Executive (Chair), Chief Finance Officer, Data Protection Officer or Deputy, Assistant Director for Digital, Data and Technology, and all Assistant Directors across the Council.

The Board met bi-monthly, with data security forming a standing item on the agenda and regular reporting provided by the Data Protection Officer and the Assistant Director for Digital, Data and Technology.

The overarching remit of the Board is to support the Council in fulfilling its statutory obligations and monitoring risk in respect of information governance and cyber security. This includes ensuring the appropriate protection of both paper and electronic data, and promoting awareness across the organisation so that all staff with authorised access to data understand and comply with 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 Freedom of Information Internal Audit

3.1 During Quarter 4 of 2025/26, an internal audit review of Freedom of Information (FOI) and complaints handling arrangements was undertaken by BDO. Audit fieldwork was completed between March and April 2026, with the final report issued in May 2026.

3.2 The scope of the audit, in relation to FOI, focused on providing assurance over the Council's compliance with the Freedom of Information Act 2000. This included a review of the policies and procedures in place; testing a sample of FOI requests to assess whether responses were provided within statutory timescales and in

accordance with legislative requirements; consideration of the application of exemptions; and a review of arrangements for identifying and monitoring requests, including those submitted via external platforms.

3.3 The outcomes and associated management actions arising from this audit will be monitored and reported during Quarter 1 of 2026/27. Overall, the report concluded Substantial Assurance on design and moderate assurance on effectiveness.

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 and updated in 2024/25. This remains the method of providing data protection training to Council Officers for 2025/26. Officers are required to complete the training on induction and annually thereafter.

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 or for new members as part of induction training. This recording remains available for Members should they wish to revisit the training at any time.

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 During 2025/26, formal meetings of the Nottinghamshire Information Officers' Group (NIOG) have reduced; however, the Council has continued to engage with information governance colleagues across Nottinghamshire through Local Government Reorganisation (LGR) workstreams. Representatives who previously attended NIOG have instead participated in LGR-focused information governance meetings to support collaborative arrangements and ensure consistency of approach across authorities.

Historically, the group has supported the Council in establishing appropriate data sharing arrangements, including the use of a standard GDPR-compliant template. Nottinghamshire County Council also maintains a MS Teams group and SharePoint site, which continues to provide a shared resource for documents, guidance, and previously agreed materials, supporting ongoing information sharing and collaboration where required.

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 2025/26 the Council received 1063 requests for information made up of 180 EIR requests, 34 DPA subject access requests, 138 DPA exemption requests and 711 FOI requests. This is slight increase when compared to the number of requests received in 2024/25 (1020).

5.3 In 2025/26 there were 2 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 2026/27.

6.2 The Data Protection Policy was updated and approved by SLT on 21 December 2022 this is to be reviewed along with the Records and Retention Policy in 2026/27.

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 was approved in 2025/26. This will ensure a standardised approach to confirming the identity of customers prior to any personal information being disclosed.

6.4 A new Artificial Intelligence Policy was also approved by Cabinet in 2025/26 to provide information on how AI can and should be used safely.

7 Information/Security Incidents

7.1 In 2025/26, the Council has recorded 45 data breaches/incidents by council officers. Of the 45 reported breaches 36 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 52 cyber security incidents last year.

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 2025/26

- ICT officers continue to be active members of the East Midlands Government Warning, Advice and Reporting Point (EMGWARP).
- Maintained Payment Card Industry Data Security Standard (PCI DSS) compliance.
- Refreshed Councillors devices with up-to-date tablets and PCs.
- Refreshed backup arrangements.
- Refreshed virtualization environment.
- Continued Windows Server refresh.
- Conducted IT Disaster Recovery Rehearsal.
- Conducted a Business Continuity rehearsal based on a cyber scenario.
- Migrated our Intranet to new platform.
- Continued to migrate legacy systems to the cloud.
- Implemented storage encryption.
- Started work on a new more detailed Cyber Risk Register.
- Increased engagement with the Business Design and Technology Authority to align procurement and system changes to enable better governance.
- Secure roll out of Whitespace and CRM Netcall.
- Records of Processing Activity have been produced for each Service Area to replace IARs.
- Employed an Information & Governance Support Officer to assist with information requests monitoring and compliance.
- Reduced the number of information requests with responses exceeding statutory deadlines.
- Approved an Artificial Intelligence Policy.
- Approved an Identification and Verification policy and procedure.

- Departmental Business Continuity plans were updated.
- Updated the Cyber Risk Register.

9 Plans for 2026/27

The following activity is planned for 2026/27:

- 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.
- 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.
- Maintain PCI DSS Compliance.
- Continue to develop the cyber security risk register.
- Implement phishing exercises and other email security improvements.
- Conduct IT Disaster Recovery Rehearsal and implement recommended actions.
- Continue to replace Servers as required and other end of support software
- 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.
- Provide targeted guidance and training to FOI responding officers to ensure all elements of requests are fully responded to and where data is publicly available that adequate information is provided to enable access to that information.
- Further guidance to be provided on FOI response templates to ensure correct templates are used and where exemptions are applied clear reasons are given in line with templates.
- Ensure continued compliance with GDPR in terms of breach reporting, DPIAs.
- Replace network switches in the Civic Centre.
- Ongoing work to implement CRM and Whitespace to ensure the Council is in a strong position moving into LGR.
- Continue to actively engage with the Local Government Reorganisation (LGR) Information Governance group, working collaboratively with partner authorities to support a smooth transition to the new authority arrangements and to ensure robust, lawful, and consistent data sharing practices are established and maintained.

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 corporate risk register also includes two strategic risks of IT/Technology and Information data which are tracked and reported to Audit Committee. Presentations have been given to Audit Committee in relation to cyber security and regular updates on activities will continue to be provided to Committee in 2026/27.

11 Conclusions

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.