Public Document Pack

Democratic Services

Civic Centre, Arnot Hill Park
Arnold, Nottingham NG5 6LU

Main number: 0115 901 3901

Please ask for: Democratic Services
Direct Dial: 0115 901 3910
Date: 26 September 2024

Dear Councillor

CABINET - THURSDAY 3 OCTOBER 2024

I am now able to enclose the following reports for the agenda of the Cabinet due to take place on Thursday 3 October 2024

Agenda No	Item
6.	**Senior information risk owner (SIRO) report (Pages 3 - 13)**

Yours sincerely

Democratic Services
Encs

This page is intentionally left blank

Report to Cabinet

Subject: Annual Report on behalf of the Senior Information Risk Owner 2023/24

Date: 3 October 2024

Author: Deputy Chief Executive

Wards Affected

Borough wide

Purpose

To present a report on behalf of the Senior Information Risk Owner providing an annual review of activities in respect of information management and data security.

Key Decision

This is not a key decision.

Recommendation

THAT:

1) The Annual Report on behalf of the Senior Information Risk Owner 2023/24 be noted.

1 Background

1.1 As Members are aware, Senior Leadership Team approved an Information Security Governance Framework setting out the Council's approach to information and cyber security risk which was endorsed by Cabinet on 1 August 2019.

1.2 The Council's designated Senior Information Risk Owner (SIRO), currently the Deputy Chief Executive and Monitoring Officer, has overall responsibility for the Council's information management framework and acts as the champion for information risk within the Council. The SIRO is currently supported by the Data Protection Officer, Deputy Data Protection Officer,

and the ICT Research and Development Manager. The SIRO is responsible for producing an Annual Report on information governance. The Annual Report has been prepared on behalf of the SIRO and is attached at Appendix 1. The report provides an overview of activity in relation to information governance, key achievements during 2023/24 as well as outlining work planned for 2024/25. It should provide assurance that the Council has arrangements in place to ensure information risks are being managed effectively.

1.3 It is important that the Council recognises the need to protect its information assets from both accidental and malicious loss and damage. The loss or damage of information can have serious consequences for the Council; not only financial and reputational but also may result in the Council being unable to deliver vital services to customers. As a result, Information Governance must be taken very seriously by the Council and this is evidenced by the on-going work activity to ensure the management and security of our information.

1.4 The Council has recently been audited by internal auditors in relation to its processes and procedures in relation to Information management. The auditors gave moderate assurance in relation to design and effectiveness with recommendations which have been included within the report attached as actions for 2024/25.

1.5 Cabinet will recall that in March of this year the Council's Digital, Data and Technology Strategy was approved, in addition, there has been a senior management restructure with investment into management positions to implement Transformation and provide management support to ICT. This investment in transformation and the recognition of its significance in driving the Council forward has to be supported by a solid governance framework in relation to ICT and data security. Work for 2024/25 is focused on strengthening cyber resilience and improving risk management in these areas. The establishment of the Business Design and Technology Authority, a body of officers that oversees requests for system changes and implementation has data security as one of its key principles when reviewing projects. This provides further oversight and a more joined up way of ensuring systems procurement has data security at its core.

2 Proposal

2.1 It is proposed that the Annual Report of the SIRO 2023/24 at Appendix 1 be noted.

3 Alternative Options

3.1 Not to present an annual SIRO report, in which case Executive members will not be updated on information governance activity across the Council and understand whether information risks are being managed effectively.

4 Financial Implications

4.1 There are no financial implications directly arising from this report.

5 Legal Implications

5.1 The Council must comply with a number of statutory obligations in the General Data Protection Regulations, Data Protection Act, Freedom of Information Act and Environmental Information Regulations. Whilst changes to legislation are expected, timelines for changes are unclear. Work for 2024/25 reflects recommendations from audit in terms of information and data and a review of training in both these areas is to be reviewed in 2024/25.

6 Equalities Implications

6.1 There are no equalities implications directly arising from this report.

7 Carbon Reduction/Environmental Sustainability Implications

7.1 There are no carbon reduction/environmental sustainability implications directly arising from this report.

8 Appendices

8.1 Appendix 1 – Annual report of the Senior Information Risk Officer 2023/24

9 Background Papers

9.1 None identified.

10 Reasons for Recommendations

10.1 To ensure the Executive is updated in respect of the Information Governance activity across the Council in order to provide assurance that information risks are being managed effectively and to ensure Information Security policy remains fit for purpose.

Statutory Officer approval

Approved by the Deputy Chief Financial Officer
Date: 25/9/24

Drafted by the Monitoring Officer
Date: 25/9/24

ANNUAL REPORT OF THE SENIOR INFORMATION RISK OWNER 2023/24

1. Purpose of this report

1.1 This report provides a summary of Information Governance activity across Gedling Borough Council during 2023/24 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 2023 to 31 March 2024; 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 2023/24.

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.
- 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 The Council has a Data Security Group (DSG) in place, the membership of which comprises the Deputy Chief Executive (Chair), Chief Finance Officer, Data Protection Officer or Deputy, and the Research and Development Manager (IT Support). The overarching remit of the group is to assist the Council to fulfil its obligations 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. Information Governance/Security Training carried out

3.1 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 2023/24. Training will continue to be delivered in this was during 2024/25 but a new updated training package will be introduced by the DPO and Deputy DPO.

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.

3.2 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.

3.3 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. This training is to be updated in 2024/25. In terms of staff without IT access who do not process large amounts of personal data, training leaflets are provided.

3.4 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.

3.5 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 was promoted during 2023/24.

4. Information Governance/Security Policy Review

4.1 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.

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

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.

6. Information/Security Incidents

6.1 In 2023/24, the Council has recorded 52 data breaches/incidents by council officers. Of the 52 reported breaches 41 were confirmed to be personal data breaches. One breach was reported to the ICO and involved an breach by an external supplier who also reported the breach to the ICO. After investigation the ICO closed the reported breach with no further action.

6.2 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.

6.3 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 DSG minutes are shared with Senior Leadership Team. No systemic failures have been identified.

6.4 IT investigated 38 cyber security incidents last year. We are not aware of any successful Cyber Security Incidents involving Malware or Hacking in 2023/24.

6.5 52% 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.

7. Summary of key achievements in 2023/24

7.1 The key achievements in 2023/24 are as follows:

- Developed the Digital Data and Technology Strategy 2024-27 with the assistance of external consultants.
- ICT officers continue to be active members of the East Midlands Government Warning, Advice and Reporting Point (EMGWARP).
- Replace or upgraded all Windows Server 2012 installs.
- Achieved PSN CoCo compliance.
- Maintained Payment Card Industry Data Security Standard (PCI DSS) compliance.
- Completed Windows 10 upgrade to version 22H2 and did initial research for Windows 11
- Migrated Office 2016 to Office 365.
- Upgraded the vulnerability management system.
- Started projects to upgrade legacy telephone lines and 3G mobile connections.
- Completed a DR rehearsal
- 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.
- Established 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.
- GDPR mandatory training continues to be available to all staff.
- New Risk management Strategy and Framework was approved by cabinet.

8. Plans for 2024/25

8.1 The following activity is planned for 2024/25:

- 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
- Replace network switches in the Civic Centre.
- Refresh backup infrastructure with newer software and hardware

- 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 Department for Levelling Up, Housing and Communities (DHCLG) related to the Local Government Cyber Assessment Framework
- Public Sector Network (PSN) compliance to be maintained.
- Maintain PCI DSS Compliance
- Improve 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.
- Implement a change from the current Information Asset Registers (IARs) to Records of Processing Activities (RoPA) to contain more detail about the personal data held by the Council.
- To explore options for a new RoPA system to be delivered through the Council's Transformation Strategy
- To update the virtual GDPR training to be delivered to staff to include more detailed information about the use of DPIA's.
- Deliver additional DPIA training to identified officers.
- 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, updating IARs and ensuring privacy notices are up to date.

9. Risk

9.1 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.

9.2 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. Work is underway to transfer risks from the old strategy to the new. Among the outstanding actions is the development of the cyber risk register which is now planned for 2024/25.

9.3 The corporate risk register also includes a risk of '*Failure to react to changes in legislation',* under which the progress to ensure compliance with the General Data Protection Regulations and Data Protection Act 2018 has been tracked. An audit of the Council's Information governance is due to be undertaken in quarter 3 of 2023/24.

9.4 A further IT cyber risk audit was completed in March 2023. The findings were reported to the Audit Committee during private session in July 2023, and are being progressed.

10. Conclusion

10.1 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.

10.2 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.

10.3 Pressure and demand on ICT continues to grow, which presents a risk to maintaining appropriate security arrangements. A new, Digital, Data and Technology Strategy will start being implemented in 2024/25.

This page is intentionally left blank