log

ANNUAL REPORT OF THE SENIOR INFORMATION RISK OWNER 2021/22

1. Purpose of this report

1.1 This report provides a summary of Information Governance activity across Gedling Borough Council during 2021/22 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 2021 to 31 March 2022;
- 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 2022/23.

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 which, if successful, will result in a significant impact on the Council's customers, staff and reputation. The more the Council relies on information technology the greater the impact.

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 Director

of Corporate Resources and s151 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: Litigation and Licensing.

2.6 The Council has a Data Security Group (DSG) in place, the membership of which comprises the Director of Corporate Resources (Chair), Head of Finance and ICT, 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 Prior to the COVID pandemic Data protection annual refresher training was delivered by the DPO and Deputy DPO via face to face corporate training sessions to both Members and staff across the Council. During the pandemic is was not possible to deliver training in this way. In order to maintain a training programme for data protection the DPO and Deputy DPO's created 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 2021/22 and will likely remain for 2022/23.

The DPO and Deputy are currently exploring providing a similar training package for Members to be delivered in 2022/23.

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. In addition, procuring a corporate e-learning package, to include Information Governance modules, continues to be explored.

3.4 The Council have continued to engage this year with the Nottinghamshire Information Officers' Group (NIOG), chairing and 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 Due to Covid 19 and other work pressures IT Support were unable to conduct any face to face or via Teams cyber security awareness training in 2021/22. However, training materials for new starters and as refresher training for existing staff was available on the Intranet. 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 will continue to be promoted during 2022/23.

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 planned during 2021/22 but completion has been delayed due to continuing Covid-19 response work and related backlog demands. A review of the Information Security Policy will now be presented for Cabinet consideration in 2022/23.

4.2 The current Data Protection Policy was approved by Cabinet on 28 June 2018 and amended in February 2019. An internal audit of the Council's IT Enterprise Architecture in 2021/22 recommended that the Data Protection Policy be reviewed and this will be undertaken by the DPO in 2022/23.

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 2021/22 the Council received 751 requests for information made up of 48 EIR requests, 21 DPA subject access requests, 99 DPA exemption requests and 583 FOI requests. This is a slight increase when compared to the number of requests received in 2020/21 (744).

5.3 In 2021/22 there was 1 request to review a decision to withhold information which was upheld, and no complaints were made to the Information Commissioner's Office (ICO).

6. Information/Security Incidents

6.1 In 2021/22, the Council has recorded 44 data breaches/incidents by council officers. Two breaches were reported to the ICO as after investigation a risk to the rights and freedoms of an individual was identified. Both breaches reported to the ICO were closed with no further action required.

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 the wrong addresses typed into systems which generates mail to the wrong address. Staff have been reminded to check address details or update changes to addresses before sending out mail. 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 There were no successful Cyber Security Incidents involving Malware or Hacking in 2021/22.

6.5 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. Unfortunately during the Covid-19 pandemic, there was an increase nationally in the number of phishing attacks relating to Teams,

Zoom and Covid-19 and as a result additional guidance was provided to Officers and Members.

7. Summary of key achievements in 2021/22

7.1 The key achievements in 2021/22 are as follows:

- ICT officers continue to be active members of the East Midlands Government Warning, Advice and Reporting Point (EMGWARP).
- Replaced our Citrix remote access solution with Microsoft Remote Desktop which is easier to maintain and uses Microsoft text message based multi factor authentication.
- Maintained Payment Card Industry Data Security Standard (PCI DSS) compliance.
- An internal audit on the Council's IT Enterprise Architecture was completed with all recommendation accepted and due to be implemented in 2022/23.
- Migrated all mobile devices to InTune mobile device management system (part of Office 365), to improve security of Council data and offer more features to staff.
- Replaced the majority of Android devices to newer, supported models, improving patching compliance. Also replaced a number of out of date Apple devices.
- Turned off final unsupported Windows Server 2008 machine. This is being kept as an archive of mortgage data but will not be turned on unless required thus mitigating the risk.
- Began Windows 10 devices upgrade to version 21H2, this will now become an annual update to newer versions in line with Microsoft continuous updating process.
- Implemented Anti-ransomware upgrade to anti-virus solution.
- Continued to implement next generation firewall technologies, particularly to protect web servers.
- Implemented a cloud based system for continuous external vulnerability scanning.
- Removed final parts of legacy email infrastructure.
- Replaced large parts of Civic Centre WIFI solution to ensure future support.
- Replaced out of support network switches in Jubilee House
- ICT Research and Development Manager to undertake continuous professional development to maintain cyber security certification.
- Completed review of existing Information Asset Registers and all Information Sharing Agreements.
- Completed administrative review of Information requests and updated departmental representatives accordingly.
- Adoption of the updated Contracts and Procurement Rules which specifically refer to the need for data protection clauses in contracts, where relevant.
- We seek to ensure records are deleted when appropriate which is an ongoing task.

- Guidance was provided to staff on the importance of maintaining confidentiality and GDPR compliance when working from home following the government advice to work from home where possible due to the Covid 19 pandemic.
- Development of virtual GDPR mandatory training rolled out to staff.

8. Plans for 2022/23

8.1 The following activity is planned for 2022/23:

- A review of Council's policies to ensure they remain fit for purpose, including: the Risk Management Strategy and Framework; the Information Security Policy; and the Records and Retention Policy, for presentation to Cabinet for approval.
- Replace out of support network switches in the Civic Centre.
- Remove final Windows 7 devices when Property Services upgrade the boiler control system.
- Continue to implement more controls on the next generation firewall features to improve security against hacking and malware.
- IT Service Delivery manager to complete video training course.
- Migrate web browser from Chrome to Edge. Deal with Microsoft's end of support for Internet Explorer in June.
- Migrate away from email delivery method considered legacy by Microsoft, must be done by October 2022.
- Implement automation of 3rd party patching, e.g. non-Microsoft products such as Adobe Reader.
- Refresh backup infrastructure with newer software and hardware and implement Office 365 backup and recovery following approval of service development bids to enhance cyber security and disaster recover measure
- Continue to work on replacing Windows Server 2012 machines which end support in October 2023.
- Continue to work with suppliers to remove potentially vulnerable Log4j components from their systems.
- Review Leisure Centre network with a view to improving disaster recovery position.
- Start working on replacing legacy analogue telephone lines due to Public Switched Telephone Network switch off by BT running until 2023.
- Plans to run Member Cyber Security training, possibly in partnership with the East Midlands Special Operation Unit (Police).
- Public Sector Network (PSN) compliance to be secured.
- Complete a review of cyber security risks and finalise the related risk register, including consideration of options for cyber security insurance cover.
- Conduct IT Disaster Recovery Rehearsal and implement recommended actions.
- Review Business Continuity Plans across the organisation to ensure they are fit for purpose in the event of a cyber security incident.

- Undertake cyber security emergency planning training
- Investigate Windows 11 for future roll out.
- Annual review of Information Asset Registers (IARs) to be conducted.
- Virtual GDPR training to be delivered to staff and Members.
- 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 corporate risk register also includes a strategic risk of "Failure to properly utilise existing ICT, react to technology changes, and prevent data loss". The risk registers are reviewed on a quarterly basis and updates reported to both SLT and Audit Committee. In respect of the main corporate risk: *Failure to properly utilise existing ICT, react to technology changes, and prevent data loss* , as reported to Audit Committee at the end of 2021/22, the risk rating was amber. Among the outstanding actions is the completion of the cyber risk register which is now planned for 2022/23.

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. As reported to the Audit Committee at the end of 2021/22 the risk rating was amber. There are no outstanding actions relating to information governance.

9.4 A further IT cyber risk audit is scheduled for the early part of 2022/23. The findings will be reported to Audit Committee.

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 Information governance is a corporate responsibility and should not be seen as simply the responsibility of the Senior Information Risk Owner, ICT team or Data Protection Officer. Reporting to Senior Leadership Team particularly in respect of the workload on ICT, patching situation and breaches and incidents reported, has continued during 2021/22 which has strengthened Senior Leadership Team oversight and ensured there is wider sharing and understanding of the challenges and solutions at a strategic level.

10.4 Pressure and demand on ICT continues to grow, which presents a risk to maintaining appropriate security arrangements. Recruitment took place for a new Technical Officer in 2020/21 failed to identify a suitable candidate. The budget for this post has been utilised on overtime, agency staff and other contractors to meet the requirements of what is an extensive work programme. An external review of ICT service provision to ensure the effective deployment of resources is in progress with a baseline assessment completed before the commencement of an options appraisal.