ANNUAL REPORT OF THE SENIOR INFORMATION RISK OWNER 2020/21

1. Purpose of this report

1.1 This report provides a summary of Information Governance activity across Gedling Borough Council during 2020/21 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 2020 to 31 March 2021;
- 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 2021/22.

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 on 11 September 2018. The Framework was endorsed by

Cabinet on 1 August 2019. The Director of Corporate Resources and s151 Officer was designated as the Senior Information Risk Owner (SIRO) during 2020/21 as part of the Management Restructure. 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, previously this role had been designated to the Service Manager: Legal Services. During 2020/21 as part of the Management Restructure the role of DPO was predesignated to the Legal Services Manager position. The DPO is assisted by two Deputies being the Legal Advisor: Litigation and Licensing and the Practice and Information Manager.

2.6 The Council has a Data Security Group (DSG) in place, the membership of which has changed during 2020/21 following the management restructure and which now 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 Data protection annual refresher training is usually delivered by the DPO and Deputy DPO via face to face corporate training sessions to both Members and staff across the Council. Unfortunately it has not been possible to deliver training in this way during 2020/21 due to COVID restrictions. In order to maintain a training programme for data protection the DPO and Deputy

DPO's have 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 launched in December 2020 and it has been successfully completed by approximately 60% of staff with the remainder now expected to complete it in the early part of 2021/22. The DPO and Deputy are currently exploring providing similar training package for Members to be delivered in 2021/22.

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 a Deputy DPO focusing on recognising and dealing with information requests and subject access request 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's 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. Unfortunately COVID has caused a delay in this project.

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 MS Teams. The group have assisted the Council in ensuring appropriate sharing agreements 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 meeting and also share information and documentation.

3.5 Due to Covid 19 pressures IT Support were unable to conduct any face to face or via Teams cyber security awareness training. However, training materials for new starters and as refresher training for existing staff is available on the Intranet and this is now being promoted for staff to complete. This consists of in-house training slides and a National Cyber Security Council provided online training course with a quiz. Scheduled training courses will be recommenced in 2021/22.

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 2020/21 but completion has been delayed due to resources being required for the Covid-19 response. However, an internal audit on cyber risk was completed in 2020/21 which included a review of the Information Security Policy and the arising low risk recommendations will be reflected in the final revision of the Policy which will now be presented for Cabinet consideration in 2021/22.

4.2 The current Data Protection Policy was approved by Cabinet on 28 June 2018 and amended in February 2019. No amendments have been made to the Data Protection Policy during 2020/21.

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 2020/21 the Council received 744 requests for information made up of 37 EIR requests, 20 DPA subject access requests, 86 DPA exemption requests and 601 FOI requests. This is a slight decrease when compared to the number of requests received in 2019/20 (775).

5.3 In 2020/21 there were 2 requests to review a decision to withhold information both of which were upheld, and no complaints were made to the Information Commissioner's Office (ICO).

6. Information/Security Incidents

6.1 In 2020/21, the Council has recorded 44 data breaches/incidents by council officers. No breaches were reported to the ICO as after investigation none of the breaches identified a risk to the rights and freedoms of an individual.

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 shared with Senior Leadership Team. No systemic failures have been identified. There has been one incident where Council equipment has been lost, being a mobile phone, but the risk of information loss was low and the device was not connected to the network so presents no ongoing risk.

6.4 There were no successful Cyber Security Incidents involving Malware or Hacking in 2020/21.

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 has been an increase nationally in the number of phishing attacks relating to Teams, Zoom and Covid-19 and as a result additional guidance has been provided to Officers and Members.

7. Summary of key achievements in 2020/21

7.1 The key achievements in 2020/21 are as follows:

- ICT officers continue to be active members of the East Midlands Government Warning, Advice and Reporting Point (EMGWARP).
- The Service Manager responsible for ICT now attends the Nottinghamshire Local Resilience Forum - Cyber Resilience Forum.
- Continued with improved monitoring arrangements for software patching and significantly improved our overall status.
- Maintained Payment Card Industry Data Security Standard (PCI DSS) compliance.
- An internal audit on cyber risk was completed and actions agreed for implementation, including a review of the Information Security Policy;
- Migrated web security (proxy) to new firewall enhancing the protection.
- Continued to remove Windows 7 and Server 2008 legacy systems, expected to be complete July 2021. This will leave one system running Windows 7. This relates the boiler control system and is mitigated by being switched off in IT and only turned on when in use, as well as running Antivirus software. This will be removed at the earliest opportunity when Property Services review the system.
- Most Windows 10 devices updated to version 1909, this will now become an annual update to newer versions in line with Microsoft continuous updating process.
- Migrated Anti-virus to cloud based system.
- Replace existing traditional firewall with one with next generation features and better redundancy. Continue to improve patching scope, timeliness and reporting, including looking at automation where possible.
- ICT Research and Development Manager attended MHCLG sponsored certified security training with examination to be completed in 2021/22.
- Rolled out Microsoft 365 components, Teams, Stream, OneDrive and Forms with associated security guidance provided.
- Completed review of existing Information Asset Registers and all Information Sharing Agreements.
- Completed administrative review of Information requests and updated departmental representatives accordingly.
- Progressed the review of the Council's Records and Retention Policy.
- Progressed the variation of all contracts to ensure they are GDPR compliant: this has largely been completed with only 4 contracts

outstanding. All other contracts which appear on the contracts register are now compliant with GDPR.

- Corporate Governance training on contracts was delivered at which the importance of GDPR compliant clauses was highlighted.
- We continue to ensure records are deleted when appropriate.
- 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.
- Upgrade of the Housing Needs system was completed to ensure GDPR compliance.

8. Plans for 2021/22

8.1 The following activity is planned for 2021/22:

- Further 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.
- Migrate 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.
- Remove final Windows 7 and Server 2008 devices. Mitigate remaining system to prevent threat from remaining Windows 7 devices.
- Continue to use next generation firewall features to improve security against hacking and malware.
- Review Citrix remote access solution.
- Plans to run Cyber Security training, possibly with the in partnership with the East Midlands Special Operation Unit (Police). Officers and Councillors will be invited.
- Public Sector Network (PSN) compliance to be secured.
- GA Cyber Stocktake results to be considered to identify what improvements can be made.
- 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.
- 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 2019/20, the risk rating was red with a target risk of amber. This was predominantly as a result of the need to separate the database in the Housing Needs system to secure GDPR compliance. This work was completed in 2020/21 and the assessed risk level has improved to the target risk of amber with the key action now outstanding being the completion of the cyber risk register which is planned for 2021/22.

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. The delivery of the project plan to ensure compliance was completed at the end of 2019/20 and ongoing monitoring in now in place as detailed in the actions in section 8 of the report. No outstanding risk concerns are raised.

9.4 During 2020/21 an advisory IT cyber risk audit was completed. A number of actions were accepted, the majority of which will be implemented in 2021/22 The findings have been 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 2020/21 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 however the recruitment process failed to identify a suitable candidate. A review to ensure the effective deployment of this resource is currently being completed by Head of Finance and ICT.