ANNUAL REPORT OF THE SENIOR INFORMATION RISK OWNER 2019/20

1. Purpose of this report

1.1 This report provides a summary of Information Governance activity across Gedling Borough Council during 2019/20 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 2019 to 31 March 2020;
- 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 2020/21.

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 The Director of Organisational Development and Democratic Services has been designated at the Senior Information Risk Officer (SIRO) and Senior

Leadership approved an Information Security Governance Framework on 11 September 2018. The Framework was endorsed by Cabinet on 1 August 2019. 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 on 3 May 2018, Cabinet designated the Service Manager: Legal Services as DPO with effect from 25 May 2018 with two deputies. On 1 August 2019, Cabinet agreed that these arrangements should continue.

2.6 The Council has a Data Security Group (DSG) in place which comprises the Director of Organisational Development and Democratic Services (Chair), Service Manager responsible for ICT, Service Manager responsible for Audit and Risk, 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 implementation of GDPR and the DPA in May 2018, the DPO and Deputy DPOs have delivered eight corporate training sessions to staff across the Council in relation to the new legislation, including two bespoke training sessions to those departments handling criminal records data. There has also been two rounds of training delivered to Members, most recently, following the election as part of the Member Induction Training package.

3.2 Departmental Representatives who are responsible for handling information requests also received specialist GDPR/DPA training in addition to the corporate training and newly appointed Departmental Reps receive one to one training with a Deputy DPO.

3.3 Data Protection training is mandatory for all staff and forms part of the training checklist on induction. Corporate sessions are held regularly to ensure all new starters receive the training. In addition, procuring a corporate e-learning package continues to be explored. It is intended that this will include Information Governance modules which will ensure all staff are adequately trained in relation to Information Governance and that they receive annual refresher training in line with the Council's Data Protection Policy. Due to Covid-19 there has been some delay in this project but the DPO and Deputy are currently working on an online training video with quiz for staff to undertake to ensure training is maintained for new starters and existing staff through a virtual session.

3.4 Training was delivered in 2019 to Service Managers on the preparation of Data Protection Impact Assessments, which assess the risks associated with the processing of personal data in performing various Council functions. The work to complete DPIAs for all existing processes where necessary is ongoing and where new processing activities commence DPIAs are completed. The DPO and Deputy DPO conducted a review of all Information Asset Registers held departmentally in 2019/20 and this will be undertaken annually to ensure asset registers remain up to date.

3.5 The Council have continued to engage this year with the Nottinghamshire Information Officers' Group (NIOG), hosting and attending meetings. The group have assisted the Council in ensuring appropriate sharing agreements in place using the NIOG template which is GDPR compliant.

3.6 An ethical phishing campaign was conducted in late 2018/19. Given the positive report and improved position since the previous campaign, the DSG agreed not to carry out a phishing audit in 2019/20 but to continue with the training and awareness.

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. No amendments have been made to the Information Security Policy during 2019/20, but a thorough review is planned in 2020/21.

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 2019/20.

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. The Legal Services team conducted a review of the information request process and system during 2019/20 and have improved efficiency in the logging and allocation of requests across departments to try and reduce the administrative burden on the Legal Services team.

5.2 In 2019/20 the Council received 775 requests for information made up of 39 EIR requests, 25 DPA subject access requests and 711 FOI requests. This is a decrease when compared to the number of requests received in 2018/19 (908).

5.3 In 2019/20 there was 1 request to review a decision to withhold information and two complaint to the Information Commissioner's Office (ICO). In one instance the ICO agreed with the Council's position on disclosure. The second complaint was closed with no recommended actions from the ICO.

6. Information/Security Incidents

6.1 In 2019/20, the Council has recorded 47 data breaches/incidents by council officers. Of those, only one was reported to the ICO on the basis it posed a risk to the rights and freedoms of an individual. In the reported case, the ICO were satisfied with the Council's investigation and response to the breach, and no further action has been taken. The previous years' data does not cover a full municipal year and therefore cannot be compared.

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.

6.4 During 2019/20, the Council has dealt with 2 further data security incidents. In January 2020, the Council was a victim of the Citrix Netscaler attack due to a vulnerability in a security appliance in the system. This attack affected multiple Councils and businesses globally. The hardened nature of the system prevented access to any data or internal systems and given the fact that swivel tokens had been withdrawn, the impact was significantly reduced. The system was restored to a known good backup point and blocked until an emergency patch was available and installed. The National Cyber Security Centre (NCSC) was contacted for advice and the incident was managed through the established Incident Management Team procedures, which worked well. This incident was also discussed with the ICO, but no reportable breach resulted as no personal information was accessed or lost.

6.5 In February 2020, a spear phish attack was launched against the Council; the email pretended to be someone looking for further information about a specific council service. The payload was an email link to Google forms which attempted to get an officer to type in their email address and password. Fortunately this was blocked by the web proxy due to the page category not being allowed to this member of staff at that time.

6.6 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 2018/19

7.1 The key achievements in 2019/20 are as follows:

- Members of ICT attended each of the series of Cyber Pathfinder training events run by the MHCLG and the SIRO attended the sessions focussed on strategic issues.
- 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.
- The National Cyber Security Centre Protective DNS system was implemented.
- Migrated inbound Email Protection between old and new cloud based systems, which will enhance protection with sandboxing and other improvements.
- Almost all of the Windows 7 devices were replaced or rebuilt with Windows 10, the remaining devices are only being used for specific purposes until system suppliers can be arranged to redeploy the software.
- Migrated Councillors to iPad based access which is more secure than using personal devices.

- Implemented new Configuration Management system for PCs to improve patch uptake and improve software roll out to remote devices.
- Improved monitoring arrangements for patching have been introduced with regular reporting to SLT.
- New web based Cyber Security training, provided by the NCSC was made available on the Intranet for new starters and staff who want to refresh their knowledge.
- Maintained Payment Card Industry Data Security Standard (PCI DSS) compliance.
- Revised Business Continuity Plan for ICT was approved by SLT and presented to SLT/Service Managers on 7 August 2019.
- Improvements were made to the Incident Management Team process for dealing with cyber incidents to align it with established emergency planning processes.
- The use of the gedling.gov.uk email for personal use was stopped due to increased phishing risk.
- Outlook Web Access (including the use of swivel tokens) was withdraw for staff and members as a cyber-security prevention measure. It makes it more difficult for an attacker to access to our systems without being on site or using one of our council issued devices.
- Participated in the LGA Cyber Stocktake and received an amber/ green rating.
- Completed review of existing Information Asset Registers and all Information Sharing Agreements for sharing arrangements requiring an ISA.
- Completed administrative review of Information requests and updated departmental reps 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.
- Data Protection and Cyber security training for Councillors was delivered following the 2019 election as part of the Member Induction programme.
- 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.

8. Plans for 2020/21

8.1 The following activity is planned for 2020/21:

- BDO (internal auditor) to conduct a Cyber Security Risk Assessment advisory audit.
- The removal of Windows 7 and Server 2008 to be completed.
- Windows 10 to be migrated to a newer edition due to end of support for the current version.
- Anti-virus system to be migrated to a cloud based console to improve reliability and visibility.
- The existing corporate firewall to be replaced, ideally with next generation model to enhance protection and detection, as budgets allow.
- Continue to improve patching scope, timeliness and reporting, including looking at automation where possible.
- ICT Research and Development Manager to attend and complete the government MHCLG sponsored certified security training.
- Continue to roll out Office 365 features in a secure way.
- Public Sector Network (PSN) compliance to be secured.
- A thorough review of Information Security Policy to be conducted by the DSG.
- The outstanding actions from the 2019 IT Controls audit to completed.
- LGA Cyber Stocktake results to be considered to identify what improvements can be made to improve the amber/ green rating.
- Annual review of Information Asset Registers (IARs) to be conducted.
- Virtual GDPR training to be delivered to staff.
- New revised Records and Retention Policy to be presented to Cabinet for approval.
- 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.
- Further review of Council's policies to ensure they remain fit for purpose.

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 is red with a target risk of amber. This is predominantly as a result of the need to separate the database in the Abritas Housing Needs system to secure GDPR compliance. An agreement has been reached with partners and the software provider and it is expected this work will be completed by September 2020.

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 nearing completion at the end of 2019/20. No outstanding risk concerns are raised.

9.4 During 2019/20 an IT controls audit was conducted and partial assurance given. This was not unexpected given the pressures and demands on ICT and capacity issues previously raised. A number of actions were accepted, the majority of which were completed in 2019/20; however a number of actions have a completion date which fall in 2020/21. Progress has already been reported to Audit Committee and will be subject to a follow up report in November 2020.

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 Officer, 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 improved during 2019/20 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. However a resource development bid for an additional IT Technical Officer to support the delivery of key digital projects and ensure that the robustness of cyber system security processes are maintained, was approved by Budget Council in March. This additional capacity will mitigate that risk. Unfortunately the recruitment process was delayed at the end of 2019/20 due to the Covid-19 pandemic, but will be progressed in 2020/21.