Gedling Borough Council

ANNUAL REPORT OF THE SENIOR INFORMATION RISK OWNER 2018/19

1. Purpose of this report

1.1 This report provides a summary of Information Governance activity across Gedling Borough Council during 2018/19 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 2018 to 31 March 2019;
- 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 2019/20.

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 is 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 General Data Protection Regulation and Freedom of Information Act. 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 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.
- Is responsible 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.

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 seven 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, there is currently a project underway to procure a corporate e-learning package which 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.

3.4 Training has also been delivered 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, for example a DPIA has been prepared on the use of some of the Council's computer systems such as Civica and Uniform. The DPO and Deputy DPO are currently conducting one to one meetings with Service Managers to review and train them on Information Asset Register completion.

3.5 An ethical phishing campaign was conducted in late 2018/19. Information was collected about whether links were clicked or passwords entered. The results were a significant improvement on the previous campaign, bringing us below the national average for responding to phishing. Personalised emails were sent to staff who responded to the emails as a training measure.

4. Information Governance/Security Policy review

4.1 A new Information Security Incident Management section of the Information Security Policy was approved by Cabinet on 3 May 2018 to take effect from 25 May 2018. In addition a number of minor amendments were approved by the Director of Organisational Development and Democratic Services on 25 May 2018, under delegated powers, to:

- Change references to GovCertUK, which no longer exists as a separate entity, to the National Cyber Security Council (NCSC)
- Make minor updates to the password section to correct elements of the recent domain password changes in the requirements section
- Update job titles in the Emergency Situations section

4.2 The Council's Data Protection Policy was updated following the implementation of GDPR and the DPA, the amended policy was approved by Cabinet on 28 June 2018, the policy was reviewed again and minor updates approved by the Leader of the Council on 14 February 2019. It is the responsibility of the DPO to ensure that the policy is regularly reviewed to ensure it remains fit for purpose and complies with the requirements of GDPR and the DPA. The policy is accessible to all staff on the intranet and on our website.

4.3 The Data Protection Policy complies with the requirement introduced by the DPA to have an appropriate policy document in place when processing special category data, which sets out the circumstances in which special category data would be lawfully processed.

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 2018/19 the Council received 908 requests for information made up of 62 EIR requests, 89 DPA requests and 757 FOI requests.

5.3 In 2018/19 there were 3 requests to review a decision to withhold information and 0 complaints to the Information Commissioner.

6. Information/Security Incidents

6.1 Since the implementation of GDPR in May 2018 to 31 March 2019, the Council has recorded 31 data breaches by council officers. Of those, only 2 have been reported to the Information Commissioner on the basis they posed a risk to the rights and freedoms of an individual. In both reported cases, the ICO have been satisfied with the Council’s investigation and response to the breaches, and no further action has been taken.

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 have been minor in nature and have largely been born out of clerical error, for example two letters in one envelope, or a letter sent to an address where the intended recipient no longer resides. Every incident is thoroughly investigated and wherever necessary, measures are put in place to reduce the risk of further incidents.

6.4 During 2018/19, the Council has dealt with 2 further data security incidents. One related to a suspected cyber-attack as a result of a vulnerability in a software application, which was reported to the Police and rectified by the supplier. The other related to the severing of a data cable, which was repaired within 3 working days. Both incidents were managed through the established Incident Management Team procedures.

6.5 In January 2018 a successful attack on the website of the provider of our Employee Benefits Scheme took place. This was followed by a phishing attack in October 2018 on the email address used by staff to sign up to the benefits scheme (work and home). The Council is not the Data Controller of this information, so was not liable to report to the ICO or secure the data, but did review the contract and data sharing arrangements with the supplier.

7. Summary of key achievements in 2018/19

7.1 It has been a significant year for Information Governance and, in particular, the Council's implementation plan for GDPR, which has now been largely completed. The achievements in 2018/19 are as follows:

- All departments completed Information Asset Registers (IARs)
- A number of 'bin it days' have been organised which has resulted in the deletion/destruction of significant numbers of Council records both paper and electronic, in accordance with records and retention policy
- Review and re-drafting of all Council forms where consent is captured as the basis for processing personal data
- IARs published
- Data Protection Impact Assessment training delivered
- GDPR leaflets prepared for staff and issued to Leisure, PASC and Waste officers
- DPIAs completed for high risk processing
- High risk contracts where personal data is processed identified and suppliers contacted to amend contracts
- Majority of high risk contracts involving data processing varied to comply with GDPR
- Revision of policy documents including Council's Information Security and Data Protection Policies
- Website and intranet pages updated to ensure GDPR compliance
- Data Protection Officer and two deputies appointed
- New data protection officer inbox set up to receive data breach complaints
- Breach notification form developed and reviewed, available on intranet
- Delivered Council wide and member training on Data Protection
- Privacy Notices completed for all Services
- Continued participation in the Nottinghamshire Information Officer's Group
- Continue to lead Nottinghamshire and Derbyshire RIPA group
- RIPA training delivered
- Annual RIPA report with updated policy approved by Cabinet on 11 October 2018
- Councillors no longer able to auto-forward emails from the Gedling email account to a private email account

- Public Sector Network (PSN) accreditation has been achieved which is essential for connection to government services such as DWP Housing Benefit Claims
- Maintained PCI DSS Compliance
- The annual Disaster Recovery Rehearsal conducted
- The Business Continuity Plan for ICT has been reviewed and agreed by the DSG
- Active member of the East Midlands Government Warning, Advice and Reporting Point (EMGWARP) Network
- Implemented the Secure Email Blueprint, to replace GCSX email system
- Implemented National Cyber Security Centre (NCSC) systems: WebCheck and MailCheck
- Continued to maintain technical security of network infrastructure
- Working with System Owners to ensure new systems have appropriate levels of security, relative to the sensitivity of the data held
- No infections, data loss, or significant downtime from hacking or malware have been detected
- Physical security has been reviewed as part of the project to accommodate Gedling Homes in the civic centre and appropriate measures will be put in place to ensure that data is not compromised as another partner moves into the building

8. Plans for 2019/20

8.1 Whilst the implementation of GDPR is largely complete, there are ongoing actions to carry over to next year as well as new actions as follows:

- Review of all IARs (in progress)
- Review Council's Records and Retention Policy (with Service Managers for comments)
- Complete variation of all contracts to ensure GDPR compliant
- Procurement of e-learning system to deliver Information Governance Training
- Review of current arrangements of Data Protection Officer and Deputy
- Review Data Sharing Agreements and ensure they are in place for all data sharing identified on IARs
- Deliver refresher training on GDPR to all staff
- Update procedure for handling information requests for all staff
- Implement more efficient process for handling information requests to minimise administrative burden and maximise efficiency of the IG system
- Review the role of departmental representatives to look at compliance as well as handling information requests
- Continue to ensure records are deleted when appropriate
- 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
- Revised Business Continuity Plan for ICT to be approved by SLT
- Cyber Security Risk Assessment to be completed and signed off by SLT
- Data Protection and Cyber security training for Councillors
- Maintain or enhance technical security during moves from legacy to newer systems, including from Windows 7 to Windows 10
- Implement NCSC Protective DNS web security system
- Attend Cyber Pathfinder series of national training events

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. As reported to Audit Committee, at the end of 2018/19, it is red with a target risk of amber. Actions have been identified and are in progress to reduce the residual risk rating.

10. Conclusion

10.1 The Council has made significant progress following the implementation of GDPR and DPA in May 2018. An advisory audit conducted in March of 2019 confirmed that the Council were progressing well. The ICO in 2018/19 allowed authorities some time to essentially get their houses in order to comply with the new legislation, going forward the ICO will take a much more active role in ensuring authorities comply with GDPR and the DPA. 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 evolve to meet the cyber security challenges of today, and tomorrow. .The data cable and cyber incidents have demonstrated the Council has robust processes in place and officer capability to deal with this type of unexpected event.