Southend-on-Sea Borough Council

Report of the Chief Executive

to

Cabinet

on
17 September 2019

Report prepared by:
John Williams, Executive Director (Legal and Democratic
Services and Senior Information Risk Owner (SIRO);
Val Smith, Knowledge and Information Manager, Corporate
Strategy Group

Cabinet Member – Cllr Terry

Information governance update and
Senior Information Risk Owner (SIRO) Annual Report 2018/19
Policy & Resources Scrutiny Committee

A Part 1 Public Agenda Item

1. Purpose of Report

1.1 To provide a summary of the Council's key actions in regard to information governance and management during 2018/19.

1.2 To report on opportunities and challenges in regard to information governance during 2019/20.

1.3 To comply with the requirement for the Senior Information Risk Owner (SIRO) to provide an annual report.

2. Recommendations

2.1 That the SIRO's report on Information Governance in Section 4 for 2018/19 be noted.

2.2 That the key actions taken during 2018/19, and the opportunities and challenges for 2019/20 be noted.

3. Background

3.1 The Council's Information Management Strategy was agreed by Cabinet in June 2016. The strategy sets out the Council's vision for managing information, the principles supporting the vision and the context and challenges faced by the Council.

3.2 It also describes the related governance arrangements and action plan to progress the Council's approach. It is complemented by a range of other strategies, policies and processes, notably Data Protection policies and procedures.

3.3 The Council's SIRO has overall responsibility for the Council's information management framework and acts as the champion for information risk within the Council. The SIRO for the Council is the Executive Director (Legal and Democratic Services).

3.4 The SIRO is responsible for producing an annual report on information governance. The report provides an overview of developments in relation to information governance, related work undertaken since April 2018 as well as outlining the strategic direction the Council has adopted. It should provide assurance that the Council's arrangements ensure personal data is held securely, information is disseminated effectively and that the Council is compliant with the legal framework - notably the GDPR and Data Protection Act 2018.

4.0 SIRO Annual Report – 2018-19

4.1 Leadership and Governance

4.1.1 The SIRO has to ensure that identified information threats and vulnerabilities are followed up for risk mitigation, and that perceived or actual information incidents are managed in accordance with Council's Risk Management Framework.

4.1.2 The SIRO's role is supported by:

- Two Privacy Officers (Data Controllers) - the Strategic Director of Transformation and the Head of ICT
- The Caldicott Guardian - the Director of Children's Services
- The Information Asset Owners (nominated officers)
- The Council's Data Protection Officer – Knowledge and Information Manager in the Corporate Strategy Group.

4.1.3 With regard to Cyber Security, the SIRO is supported by the Cyber Security Lead, (the Head of ICT). The ICT nominated cyber security specialists monitor developments; safeguard corporate systems and provide advice and training to the organisation concerning the responsibility of all staff to be aware of and to guard against cyber security threats. They also risk assess those aspects of Data Protection Impact Assessments which involve the use of such technology.

4.1.4 The Data Protection Officer (DPO) and their team assist the organisation in monitoring internal compliance, informing and advising on data protection obligations, providing advice, assistance and training on data protection matters and act as a contact point between the Information Commissioner and the Council. It is a statutory requirement that the DPO reports to the highest management level. Usually this is the Good Governance Group (GGG) but on occasions it will be the Corporate Management Team (on which the SIRO also sits).

4.1.5 The DPO's team also manages Data Protection and Freedom of Information central records, monitors performance and compliance with legislation and leads on records management.

4.1.6 Leadership and governance of information management was provided by the Corporate Information Governance Group (CIGG) during 2018/19. For 2019/20 this responsibility has passed to the Good Governance Group which has a revised remit, now encompassing information management along with the promotion of simple and effective governance.

4.1.7 The GGG is chaired by the SIRO, with membership including the SIRO, the Privacy Officers, the Caldicot Guardian and the DPO.

4.1.8 The Data Protection and Freedom of Information Community of Practice, led by the Knowledge and Information Manager, is a sub group of the Good Governance Group. The COP monitors performance and has a focus on sharing good practice and its members provide expert knowledge to their colleagues. The SIRO is a member of the COP.

4.1.9 The Council is a signatory to the Whole Essex Information Sharing Framework (WEISF). The associated forum has been refocused for 2019/20 and is now known as the Wider Eastern Information Stakeholder Forum. Membership assists the Council in sharing appropriate personal data with public, third sector and contracted private organisations across Essex in a lawful, safe and informed way and in its new form will collaborate on a wider range of information governance matters than simply information sharing.

4.1.10 The Council is also a member of the Essex On-line Partnership which as part of its remit supports cyber security and the Information Governance Networking Group, a collection data protection specialists who share practical advice and support in an informal environment.

4.2 Training and Awareness

4.2.1 Data Protection training continues to feature as a key part of ensuring staff are aware of their responsibilities. In 2018/19 this comprised of formal class room training, induction training and SPARK e-learning module (which was also a gateway to permission being allowed to work remotely).

4.2.2 During 2019/20 this training is being replaced by an e-learning platform. Modules covering data protection and cyber security will be mandatory for all staff handling personal data. Staff who are less familiar with the use of computer based learning will be provided with supported training. For those with minimal personal data involved in their role, alternative provision will be made to ensure that a sufficient level of understanding is reached.

4.2.3 When examining data protection security incidents, the Data Protection Advisory Service routinely consider resultant training needs and bespoke training is provided as required.

4.2.4 Messages continue to be provided to staff alerting them to the need to protect personal data and use it appropriately. These have included blogs from the Data Protection Officer, posters emphasising the value of personal data, all staff messages.

4.2.5 In addition to the above, ICT have delivered training and awareness sessions specifically relating to cyber security and regular cyber security messages are issued by ICT to staff.

4.3 General Data Protection Regulation and Data Protection Act 2018

4.3.1 The European Union General Data Protection Regulation (GDPR) came into effect on 25 May 2018. The GDPR has direct effect across all member states and is the main point of reference for most data protection legal obligations.

4.3.2 The Data Protection Act 2018 (DPA 2018) also came into effect on that date. This details UK specific provisions allowed for by the GDPR and applies similar standards to GDPR to the handling of personal data which is not covered by EU law, for example to data relating to immigration.

4.3.3 The DPA 2018 also brings the EU Law Enforcement Directive into UK domestic law. This sets out the requirements for the processing of personal data for criminal law enforcement purposes and will apply to the Council in regulatory activities which may result in criminal prosecution.

4.3.4 As national security is also outside the scope of EU law, the DPA 2018 also specifies the data protection standards to be met by the intelligence services, based on the Council of Europe Data Protection Convention 108.

The DPA 2018 also covers the duties, functions and powers of the Information Commissioner (ICO) and the corresponding enforcement provisions.

4.3.5 The GDPR and DPA 2018 must be read side by side when considering the application of data protection legislation. Requirements concerning the proper use of personal data will not change upon the exit of the UK from the EU. This is because the UK government has committed to the adoption of the provisions of the GDPR into UK law.

4.3.5 An audit of the programme of work in preparation for GDPR was concluded in January 2019. It found that a comprehensive programme of work had been undertaken in advance of GDPR. The remaining actions to embed GDPR as business as usual were identified and the resulting data protection action plan is being progressed during 2018/19, led by the Knowledge and Information Manager, with progress being overseen by the Good Governance Group.

4.4 Data Security and Protection Toolkit

4.4.1 The Data Security and Protection Toolkit is an online tool that enables organisations to measure their performance against data security and information governance requirements which reflect legal rules and Department of Health policy. The Data Security and Protection Toolkit is the successor framework to the Information Governance Toolkit.

4.4.2 This independently audited self-assessment tool enables the Council to demonstrate that it can be trusted to maintain the confidentiality and security of personal information, in particular health and social care personal records.

4.4.3 The 2018/19 IG Toolkit was successfully completed. An independent audit gave the Council assurance concerning their self-assessment, confirming that the Council has appropriate evidence available for the 'Standard Met' assessment.

4.5 Freedom of Information/Environmental Information

4.5.1 Under the Freedom of Information Act (FOIA) and Environmental Information Regulations (EIR), individuals are entitled to ask the Council for a copy of information it holds.

4.5.2 1480 requests were received in 2018/19, compared to 1238 in 2017/18. To ensure consistency and compliance the FOI/EIR function is managed corporately within the Corporate Strategy Group (CSG). Requests are recorded centrally and then dispersed to departmental specialists for collation of data and for response. Where a response requires data from multiple departments, the response is collated by CSG.

4.5.3 In 2018/19 the Council replied to 1369 requests, 76.41% within the required 20 working days. This compares to 1192 replied to in the previous year with 75.08% compliance. Consideration is being given to whether more data could be published to avoid the need for requests to be made.

4.6 Subject Access Requests

4.6.1 Under data protection legislation, individuals are entitled to ask the Council for a copy of the personal data it holds about them. This is known as a Subject Access Request (SAR).

4.6.2 There have been 75 SARs received in 2018/19 an increase from 62 in the previous year. The increase may be because there is no longer a fee for making a request.

4.6.3 82 SARs were completed in 2018/19, an increase from 64 in the previous year. Some SARs are highly complex as they involve weighing the data protection rights of multiple data subjects within a record and may involve hundreds of documents. This has made responding within the one month target (or three months for complex cases) a challenge.

4.6.4 In 2018/19 additional resource was allocated to increase the speed with which requests are processed. While there has been improvement, further work will be undertaken to investigate causes of delay and optimise case handling.

4.7 Requests for Data Sharing

4.7.1 In 2017/18 a total of 898 individual requests for data sharing were received. Such requests are mostly received from the Police, for third party information. These requests are generally received through Legal and Democratic Services, Revenues and Benefits, Counter Fraud and Investigation and the Corporate Strategy Group.

4.7.2 Requests are centrally recorded to encourage consistency in decision making and to provide an audit trail in the event of a query regarding the appropriateness of data sharing.

4.7.3 Where information sharing is a regular occurrence, the Data Protection Advisory Service continues to work with service areas to introduce formal Information Sharing Agreements to promote clarity of responsibilities between all parties.

4.8 Data Security Incidents

4.8.1 In 2018/19 no data security incidents required notification to the Information Commissioner. Of the 52 incidents identified but not requiring reporting, 46 related to information being provided to the wrong recipient.

4.8.2 The increased data protection training carried out has raised awareness within the organisation of the need to formally report data security incidents and this has resulted in an increase in the numbers investigated. Not all reported incidents will have resulted in a breach. Even where there is no breach, incidents can provide valuable insight into processes and procedures which may need to be strengthened as a preventative measure or where training is required.

4.9 Records Management

4.9.1 With increasing public access to Council records, it is important that necessary documents are retained and that records are destroyed as part of a managed process that is adequately documented. Therefore, services must have in place clearly defined arrangements for the assessment and selection of records for disposal, and for documenting this work. All record keeping procedures must comply with the Council's Document Retention and Disposal Policy.

4.9.2 The Council has an Information Asset Register which acts as a mechanism for understanding and managing the Council's information assets and the risks to them.

4.10 Information Security (including Cyber Security)

4.10.1 The Council took part in a Local Government Association Cyber Security stocktake. Following this, a cyber security action plan has been created, led by ICT with progress being overseen by the Good Governance Group.

4.10.2 Activity concerning the action plan will be supported by a sub group of the Good Governance Group with a core membership of staff from the Governance, ICT and Resilience specialisms.

4.10.3 Awareness of cyber security matters has been maintained by informal staff workshops and regular communications, led by ICT. In 2019/20 this will be enhanced by mandatory e-learning, as described above.

4.10.4 To ensure appropriate security is given to data, ICT assess cyber security risk as part of the Data Protection by Design process.

4.10.5 The cyber security threat landscape is actively monitored and emerging risk is identified and mitigated. To aid with this, intelligence is obtained from the National Cyber Security Centre - Cyber Security Information Sharing Partnership and Warning, Advice and Reporting Point (WARP) services.

4.10.6 Action is taken by ICT to continuously block malware threats to the Council's assets, such as laptops, PCs and Servers. Both preventative and reactive action is taken to manage cyber security incidents. From 2018/19 regular security reports will be provided to the Good Governance Group. Detail is not published in this report to avoid providing the means for a motivated person to attack the Council's systems.

5 Strategic Direction - Future Programme of Work

5.1.1 The primary focus for the Council in relation to information management and data protection in 2019/20 will be to progress the data protection and cyber security action plans.

5.1.2 The Council's ambitions regarding being a Digital City will be further explored and the Digital Strategy will be reviewed and revised.

5.1.3 The Good Governance Group will develop in its new role as one of the boards within the new officer governance structure.

5.1.4 Cyber security and data protection risk will continue to be actively monitored and emerging risk identified and mitigated.

5.1.5 The programme of introducing new digital infrastructure across the borough will be completed in 2019/20 providing super-fast connectivity for Council buildings, schools, businesses and homes.

6 Other Options

6.1 It is a requirement of the Council’s Information Management Strategy that an annual report is made to councillors.

7 Reason for Recommendation

To ensure that the Council holds personal data securely; disseminates information effectively; is transparent and enabling in its handling of information and operates within the necessary legal framework.

8 Corporate Implications

8.1 Contribution to Southend 2050 Road Map

Sound information management and the protection of personal data contribute to all aspects of the Southend 2050 Road Map.

8.2 Financial Implications

Any financial implications arising from this work will be considered through the normal financial management processes. Proactively managing information can result in reduced costs to the Council by reducing exposure to potential loss (such as fines from the Information Commissioner which could be up to £17million).

8.3 Legal Implications

Information management and Data Protection are subject to a range of legislation, but in particular the General Data Protection Regulation and Data Protection Act 2018, as detailed in this report.

8.4 People Implications

Any people implications will be considered through the Council’s normal business management processes.

8.5 Property Implications

None

8.6 Consultation

Internal

8.7 Equalities and Diversity Implications

Data Protection Policies and Procedures are available on the Council’s website and transactional forms are included in MySouthend. Alternative channels remain available for those customers who may not be able to access or use digital services, and reasonable adjustments for disability are made where required.

8.8 Risk Assessment

Non-compliance with the law would adversely affect the Council's reputation in the community, reduce public trust and could lead to regulatory penalties and disruption to business continuity.

8.9 **Value for Money** – None identified

7.10 **Community Safety Implications** – None identified

7.11 **Environmental Implications** – None identified

8 **Background Papers** - None

9 **Appendices** - None