Southend-on-Sea Borough Council

Report of the Chief Executive

to

Cabinet

on
14 September 2021

Report prepared by:

John Williams, Executive Director (Legal and Democratic Services and Senior Information Risk Owner (SIRO)
Val Smith, Knowledge and Data Privacy Manager, Corporate Strategy Group

Cabinet Member – Cllr Gilbert

Information Governance Update and
Senior Information Risk Owner (SIRO) Annual Report 2020/21
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 2020/21.

1.2 To report on opportunities and challenges in regard to information governance during 2021/22.

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 for 2020/21 (Section 4 of this report) be noted.

2.2 That the key actions taken during 2020/21, and the opportunities and challenges for 2021/22 be noted.

3. Background

3.1 The Council's Information Management Strategy was agreed by Cabinet in June 2016 and 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 and 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 2020 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 UK General Data Protection Regulation (GDPR) and Data Protection Act 2018.

4. SIRO Annual Report – 2020-21

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

4.1.3 With regard to cyber security, the SIRO is supported by the Head of IT Security and Compliance. 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 procurement and 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 (of which the SIRO is also a part).

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 is provided by the Good Governance Group (GGG) whose remit includes 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 Council is a signatory to the Whole Essex Information Sharing Framework (WEISF). The associated forum is known as the Wider Eastern Information Stakeholder Forum and is regularly attended by the Information Governance Advisor. Membership assists the Council in sharing best practice and in the appropriate sharing of personal data with public, third sector and contracted private organisations across Essex in a lawful, safe and informed way.

4.1.9 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 of data protection specialists who share practical advice and support in an informal environment. Additionally, the partnership plays a critical role in the Essex Resilience Forum cyber framework for Incident Response planning and exercising.

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.

4.2.2 During 2020/21 training was primarily through an e-learning platform with modules covering data protection and cyber security. For those with minimal personal data involved in their role, alternative provision is made to ensure that a level of understanding is reached appropriate to responsibilities.

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 through a variety of communication channels are provided to staff alerting them to the need to protect personal data and use it appropriately.

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 On the UK's exit from the EU on 31 December 2020, the UK GDPR and an amended Data Protection Act 2018 (DPA 2018) became the primary pieces of legislation regulating data protection in the UK.

4.3.2 Following the changes, key data protection principles, rights and obligations have remained the same, but the UK has the independence to keep its data protection framework under review.

4.3.3 Countries in the European Economic Area (EEA) remain subject to the EU GDPR and EU Law Enforcement Directive. To allow data to continue to flow without additional safeguards, a temporary arrangement known as 'the bridge' was agreed pending an 'adequacy decision'.

4.3.4 On 28 June 2021 EU-UK adequacy decisions were published by the EU Commission designating the UK as adequate (and able to be sent data without additional safeguards). There are exceptions for immigration data. The adequate designation is expected to last until 27 June 2025 with a possible maximum extension of four years. The EU will monitor data protection developments in the UK and adequacy could be withdrawn if it was considered appropriate.

4.3.5 Throughout this process, the adequacy position and the possible implications for the Council's data flows has been monitored by the data protection service, updating the Council's EU Exit group and Good Governance Group as required.

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 Toolkit requires the Council to measure its performance against the National Data Guardian's 10 data security standards.

4.4.2 All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security, that personal information is handled correctly, and they can consequently be trusted to maintain the confidentiality and security of personal information, in particular health and social care personal records.

4.4.3 The 2020/21 Toolkit was successfully completed. The Toolkit requires an independent audit of the Council's self-assessment. This was conducted in May 2021 with the outcome that there is substantial assurance that the necessary standard is met.

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.

4.5.2 962 requests were received in 2020/21, compared to 1227 in 2019/20. The number of requests received declined sharply during the first six months of the pandemic but are now increasing almost to previous levels).

4.5.3 In 2020/21 the Council replied to 926 requests, 69% within the required 20 working days. Although the volume of requests declined because of the pandemic, so too did officer availability to source data for the responses, primarily because of altered priorities, staff absence and redeployment.

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 were 79 SARs received in 2020/21 and 81 were completed. 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. Responding within the required one month (or three months for complex cases) continues to be a challenge.

4.7 Requests for Data Sharing

4.7.1 In 2020/21 a total of 358 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 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 works 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 2020/21 no data security incidents required notification to the Information Commissioner.

4.8.2 All reported incidents are investigated. Even where there is no breach, incidents can provide valuable insight into training requirements and processes and procedures which may need to be strengthened as a preventative measure.

4.9 Information Security (including Cyber Security)

4.9.1 The enhanced organisation of the security function and operating model introduced in 2019/20 as part of the restructuring of the ICT service continues to offer the necessary support to the organisation.

4.9.2 A cyber security strategy for SBC was presented and approved by the Good Governance Group in October 2020 and the head of ICT and IT Security and Compliance provide updates and reports to the Good Governance Group at each meeting.

4.9.3 During the reporting period there have been significant technology changes and uplifts which have enhanced the Council's security capabilities, for example:

- Microsoft Enterprise Licensing uplifted to the most comprehensive E5 Security services and tools.
- Laptop and Desktop modernisation and standardisation with enhanced security lockdown and controls.
- Upgraded email and web content filtering and threat protection.
- Enhanced encryption on devices and email.
- Ransomware containment solution, currently in delivery and testing.
- Enhancements to identity and access security and associated monitoring.

4.9.4 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 (NCSC), Cyber Information Sharing Partnership (CISP) and Warning, Advice and Reporting Point (WARP) services.

4.9.5 Through the Local Government Association (LGA), Essex Online Partnership (EOLP) and NCSC networks, the Council has had the opportunity to capitalise on grants, and funded initiatives as well as the full suite of NCSC services, for example:

- LGA grant for Cyber Security training and certification
- Metacompliance Phishing simulations and learning materials
- Network Early Warning System – vulnerability scans by NCSC

4.10 Records Management

4.10.1 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.

4.10.2 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.

5. Strategic Direction - Future Programme of Work

5.1.1 The COVID-19 pandemic is expected to continue to affect information governance priorities during 2021/22.

5.1.2 Reliable and secure remote access to Council systems remains a necessity as is video conferencing which is now is a regular feature of working lives.

5.1.3 Supporting the data protection element of new roles and responsibilities arising from Coronavirus activities continues to be of importance.

5.1.4 Arrangements for the handling of data protection support, Freedom of Information and Subject Access Requests will be reviewed as part of the Business Support redesign process.

5.1.5 Through 2021/22 ICT will continue to focus on adoption of Microsoft 365 technologies, along with the security and information governance improvements this will bring. Continuation of cloud first ICT and application migration to Azure will also bring cyber and data security benefits. Cyber resilience plans will be exercised to ensure we have prepared for emergency and crisis situations.

5.1.6 Following the May 2021 local elections all councillors were provided with specific cyber security briefing and skills workshops. All staff have received email Phishing attack simulations to exercise and educate staff on the risks presented through email based attacks.

5.1.7 A report to Audit Committee covering in more detail all aspects of the Council's cyber programme risks and developments is in production.

5.1.8 An independent assessment of the Council's cyber security capabilities took place in July 2021. This was by an external company on behalf of Internal Audit and once finalised will be reported through the relevant democratic process.

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

7.1 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

Many aspects of the Southend 2050 Road Map will be underpinned by technology and data. Sound information management and the proper protection of personal data therefore contributes to all aspects of the Southend 2050 work. Providing reliable information management which is trusted will contribute to the safety of residents and enabling technological advancements will contribute to making Southend a leading digital city.

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, including the UK General Data Protection Regulation and Data Protection Act 2018as amended, 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

8.10 **Community Safety Implications** – None identified

8.11 **Environmental Implications** – None identified

9. Background Papers - None

10. Appendices - None