Southend-on-Sea City Council

Report of the Chief Executive

to

Audit Committee

on

26 October 2022

Report prepared by:

Stephen Meah-Sims, Executive Director - Strategy, Change and Governance and Senior Information Risk Owner (SIRO)

Val Smith, Knowledge and Data Privacy Manager, Corporate Strategy Group

---

Information Governance Update and
Senior Information Risk Owner (SIRO) Annual Report 2021/22

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 2021/22.

1.2 To report on opportunities and challenges in regard to information governance during 2022/23.

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 2021/22 (Section 4 of this report) be noted.

2.2 That the key actions taken during 2021/22, and the opportunities and challenges for 2022/23 be noted.

3. Background

3.1 The Council's Information Management 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 is complemented by a range of other strategies, policies, and processes, notably Data Protection policies and procedures.

3.3 The Council's Senior Information Risk Owner (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 for Strategy, Change and Governance.

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 2021 as well as outlining the strategic direction the Council has adopted. It provides 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 – 2021-22

4.1 Leadership and Governance

4.1.1 The SIRO has a responsibility 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:

- The Privacy Officer - the Director of Digital and ICT
- The Caldicott Guardian - the Director of Commissioning
- The Data Protection Officer – the Knowledge and Data Privacy Manager
- Information Asset Owners (nominated officers).

4.1.3 With regard to cyber security, the SIRO is supported by the Director of Digital and 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 risk 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. The DPO acts as a contact point between the Information Commissioner and the Council. It is a statutory requirement that the DPO has a reporting line 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 a member).

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 Officer, 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 known as the Wider Eastern Information Stakeholder Forum is attended by the DPO or their delegate. 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 Digital 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 2021/22 training at induction was through an e-learning platform with modules covering data protection and cyber security. The 2021/22 annual data protection training exercise for staff focused on key areas of the practical application of data protection legislation:

- The requirement for data protection risk assessments
- The definition of personal data
- Identifying data subject rights requests
- How to handle a suspected data breach
- Keeping personal data safe

The training was graduated to ensure that an appropriate level of understanding was reached proportionate 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. These include several Phishing attack simulations to everybody using Council email, and accompanying training and awareness related to these attacks.

4.3 UK General Data Protection Regulation and Data Protection Act 2018

4.3.1 The UK GDPR and Data Protection Act 2018 (DPA 2018) are the primary pieces of legislation regulating data protection in the UK.

4.3.2 Key data protection principles, rights and obligations have remained the same as they were under the EU GDPR, but the UK has the independence to keep its data protection framework under review. So far the UK government has not chosen to make changes but has been considering its options. The situation continues to be monitored by the DPO, who will update the Council's EU Exit group and Good Governance Group if required.

4.3.3 On 28 June 2021 EU-UK adequacy decisions were published by the EU Commission designating the UK as adequate (and able to share personal 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.

4.4 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 enables 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. Without the Toolkit assurance, NHS organisations would be unlikely to share data with the Council.

4.4.3 The 2021/22 Toolkit was successfully completed. The Toolkit requires an independent audit of the Council's self-assessment. This was conducted in June 2022 with the successful 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 which is of interest to them.

4.5.2 993 requests were received in 2021/22, compared to 962 in 2020/21. The number of requests received, having declined sharply during the first six months of the pandemic in 2020 have now returned to previous levels.

4.5.3 In 2021/22 the Council replied to 1031 requests, 59% within the required 20 working days. It is recognised that the timeliness of reply needs to improve. An aim of the business support review is to bring together in one area officers who administer the FOI process so that a sharper focus can be given to this area of work and solutions found to the causes of delays.

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 130 SARs received in 2020/21 in a return to pre-pandemic levels. 92 were completed, 42.39% within the required timescale. 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.

4.6.3 Responding within the required one month (or three months for complex cases) continues to be a challenge. An aim of the business support review is to bring together in one area officers who administer the SAR process so that a sharper focus can be given to this area of work and solutions found to the causes of delays. In particular, following suitable training a wider pool of staff will become available to assist with peaks of work and complex cases.

4.7 Requests for Data Sharing

4.7.1 Individual requests for data sharing are received, primarily from the Police, for the sharing of 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 2021/22 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 cyber security strategy for SBC continues to set the direction for continuous improvement and overall approach to cyber risk management. The head of ICT and IT Security and Compliance provide updates and reports to the Good Governance Group at each meeting. These have provided regular updates on the threat landscape, containing information relevant to the Council including that provided through National Authority, the NCSC. In particular relevant changes in threat in light of the ongoing Ukraine invasion by Russia.

4.9.2 Since the last annual report there have been significant technology and process changes and uplifts which have enhanced the Council's security capabilities, for example:

- Utilising the Microsoft Enterprise Licensing to enhance various controls and mitigate risks:
    - Migration of data to secure, monitored cloud facilities
    - Enhancements to Web Content Protection and Filtering
    - Enhanced email protection for attachments and URLs in messages
    - Protection of applications and data accessed from personal devices in line with Bring Your Own Device Policy
    - Cloud Application Risk Assessment and Controls deployed
- Updated Policies to support Hybrid and Remote Working as well as use of Mobile Phones and Personal Devices.
- Completion of Ransomware containment solution.
- Continuation of migration of applications and data to more secure, monitored cloud computing environments.
- Enhanced use of data for reporting, and analysis of asset and vulnerability.

4.9.3 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.

4.9.4 Through the Department for Levelling Up Housing & Communities(DLUHC), Local Government Association (LGA), Essex Digital Partnership (EDP) 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

- Police Cyber Alarm
- DLUHC Cyber 360 and Cyber Assessment Framework participation and funding

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 and a Record of Processing Activities (RoPA) which details the many purposes for which data is processed by the Council and associated retention requirements.

5. Strategic Direction - Future Programme of Work

5.1.1 The COPI (Control of Patient Information) emergency measure enabling greater sharing of healthcare data to support the management and mitigation of the spread and impact of the current outbreak of Covid-19 ended after two years on 30 June 2022.

5.1.2 This means that the council can no longer rely on COPI as a justification for processing data and must stop any processing which relied solely on the emergency measure. In practice, most of the Council's data is processed under alternative legal authorisation.

5.1.3 However, particularly regarding public health data, it has been necessary to ensure that data collected for the purpose of Test and Trace and support during the pandemic for vulnerable people is appropriately cleansed. This work has been carried out by the service in consultation with the Director of Public Health and the Data Protection Officer.

5.1.4 As mentioned above, arrangements for the handling of data protection support, Freedom of Information and Subject Access Requests will change in late 2022 as a result of the Business Support review. The Information Governance, Complaints and Resolution Hub within the new Customer Support Service will centralise services for FOI, EIR and SAR requests. Once established, it is anticipated that there will be improved resilience and a sharper focus on these areas. Once trained, a wider pool of staff will be available to smooth peaks of work. Enhanced reporting will be provided to services required to provide information in connection with requests, enabling issues causing delays to be identified and remedied. In combination, over time, this is expected to improve response times for FOI, EIR and SAR requests.

5.1.5 The data protection advisory service will also be encompassed within the Information Governance, Complaints and Resolution Hub towards the end of 2022. Policies and procedures will be updated to reflect the change.

5.1.6 Through 2022/23 ICT will continue to focus on adoption of Microsoft 365 technologies and the migration of existing data and applications to more secure, monitored cloud computing environments. Cyber resilience plans that have been drawn up will be exercised to ensure the Council is prepared for emergency and crisis situations.

5.1.7 The Council are one of eight local authorities participating in the Cyber Assessment Framework (CAF) Pilots and it is anticipated that this will be placed at the centre of future planning for cyber assessment and continuous improvement towards achieving and maintaining the standards set for local authority cyber in the UK.

5.1.8 Following the May 2022 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.

5.1.9 An independent assessment of the Council's cyber security was completed in late 2021. This was by an external company on behalf of Internal Audit. A report has been provided to Internal Audit and shows a marked increase in ICT and Cyber Security capability and maturity.

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 2018 as 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