Southend-on-Sea City Council

Agenda Item No.

Meeting:	Audit Committee
Date:	25 October 2023
Classification:	Part 1
Key Decision:	No
Title of Report:	Information Governance Update and Senior Information Risk Owner (SIRO) Annual Report 2022/23
Executive Director:	Michael Marks, Children and Public Health
Report Author:	Michael Marks, Children and Public Health, Senior Information Risk Owner (SIRO) Val Smith, Customer Service Manager, Information, Complaints and Resolution
Executive Councillor:	Cllr Cox: Leader (Cabinet Member for Special Educational Needs & Disability)

1. Executive Summary

1.1. This report provides a summary of the Council's key actions in regard to information governance and management during 2022/23. It provides a summary of the opportunities and challenges with regard to information governance during 2023/24 and satisfies the requirement for the Senior Information Risk Owner (SIRO) to provide an annual report.

2. Recommendations

2.1 It is recommended that the Committee:

a. Note the report of the Senior Information Risk Owner on Information Governance for 2022/23.
b. Note that the Council has the necessary structures in place to manage information lawfully as demonstrated by the compliance with the Data Security and Protection Toolkit and cyber security audits.
c. Note that officers have good external networks ensuring good practice is shared regionally and implemented within the Council.
d. Note that in response to the Corporate Peer Review the Council has introduced a Governance Board as a means of providing oversight of the information framework.
e. Recognise that training and awareness tools are available to officers and members however participation while adequate could be improved and the Governance Board will be asked to improve the cascade of training throughout the organisation.

f. Note that the fulfilment of Freedom of Information/Environmental Information requests and Subject Access Requests requires improvement and to further note the Governance Board will be asked to drive improvement across the organisation.
g. Note that officers across the Council are participating in a major drive to move information to a better structured and more secure environment as part of the Shared Data Migration project led by ICT.

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 currently the Executive Director, Children and Public Health who has been covering the role temporarily since the departure of the Executive Director for Strategy and Change in July 2023. The SIRO role will be reassigned in the near future.

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 2022 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 2022/23

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 Executive Director, Adults and Communities

- The Data Protection Officer – the Customer Support Manager, Information Governance, Complaints and Resolution.
- 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 teams 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 Governance Board but on occasions it will be the Corporate Leadership Team.

4.1.5 The DPO's teams also manage Data Protection, Freedom of Information and Subject Access Request central records, monitor performance and compliance with legislation and lead on records management.

4.1.6 Leadership and governance of information management is provided by the Governance Board whose remit includes but is not limited to information management and the promotion of simple and effective governance.

4.1.7 The Governance Board membership includes the SIRO, the Privacy Officer, the Caldicot Guardian, the Head of Internal Audit and Counter Fraud 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 (Essex), 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.

4.1.10 The Council is represented on the Mid and South Essex Integrated Care System (ICS) Information Governance Steering Group.

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 2022/23 training for both existing staff and upon induction for new staff was through an e-learning platform with modules covering data protection and cyber security. 96 % of staff have completed Data Protection training and 89% Cyber Security training. Tailored training for Councillors was provided through an online presentation and an accompanying briefing document. 14 Councillors attended the presentation, and all Councillors were provided with the briefing document for their information.

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. This year 28 separate communications have been provided concerning guidance on the use and securing of personal data. A further 16 communications were shared related to cyber security.

4.2.5 Several Phishing attack simulations have been delivered to everybody who uses Council email. Where users are compromised as a result of the simulation, additional training is provided. In the most recent exercise 12 of those compromised have completed their training (60%).

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. In June 2022 the UK Government first published its plans to reform the UK Data Protection Act. In March 2023 the Data Protection and Digital Information Bill was introduced and is currently going through the House of Commons. The situation continues to be monitored by the DPO, who will update the Governance Board 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 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 2022/23 Toolkit was successfully completed. The Toolkit requires an independent audit of the Council's self-assessment. This was conducted in June 2023 with the successful outcome that there is substantial assurance that the necessary standard is met.

4.4.4 The Key Findings of the Audit were:

- Good governance structure including clear lines of responsibility and accountability from the senior team and Governance Board.
- Key Roles implemented – SIRO, Caldicott Guardian and Data Protection Officer.
- Policies reviewed and up to date.
- Website clear and transparent about uses of information – Privacy Notices, Policies, Information Sharing, National Data Opt-Out, individual Rights & Subject Access Requests.
- Good level of staff training in Data Protection and Cyber Security.
- Starters / Movers and Leavers processes embedded with removal from Active Directory.
- Business Continuity Plan that includes Data and Cyber Incident response.
- Due diligence against suppliers, partners.

4.4.5 It was recommended that the Caldicott Guardian carry out specialist training and be added to the National Caldicott Guardian Register.

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 1196 requests were received in 2022/23, compared to 993 in 2021/22.

4.5.3 In 2022/23 the Council replied to 1099 requests, 66.15% within the required 20 working days. This is an improvement on the 59% achieved the previous year but still needs to improve considerably. At the request of the Performance Board increased reporting to management teams is being introduced to improve awareness and accountability of outstanding requests. Information and training will be provided throughout the organisation, ranging from general awareness for all staff to more in-depth training for those likely to be responding to, or providing information for, requests on a regular basis.

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).

4.6.2 132 requests were received in 2022/23, compared to 130 in 2021/22. 120 were completed an increase of 30% over the previous year. However clearing older cases has resulted in a low rate of 29.17% being completed within the required timescale..

4.6.3 Responding within the required one month (or three months for complex cases) continues to be a challenge. Some SARs are highly complex as they involve weighing the data protection rights of multiple data subjects within a record and may involve hundreds or even thousands of documents. Following the business support review in November 2022 officers who administer the SAR process have been brought together as part of a larger team. This has enabled additional officers to assist the core officers on an as-and-when basis. This is enabling a greater number of SAR to be processed each month as the drive to get this area of work up to date continues.

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 Customer Services (Information Governance, Complaints and Resolution).

4.7.2 Requests are centrally recorded to provide an audit trail in the event of a query regarding the appropriateness of data sharing. Forty requests were recorded in 2022/23. Each request is considered on its merits and information is only shared where there is a legal basis to do so.

4.7.3 Where information sharing is a regular occurrence, the Information Governance, Complaints and Resolution 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 2022/23 no data security incidents were of a severity where the risk required notification to the Information Commissioner.

4.8.2 44 breaches of data protection legislation were identified. These consisted of:

- 22 communications sent to the wrong recipient (18 email, 4 letter).
- 9 incidents of incorrect sharing of information.
- 5 instances where data was not fully redacted in documents.
- 3 occasions when information was inappropriately added to the Council's website
- 5 Other

4.8.3 All reported incidents are investigated, and mitigating action taken where necessary. 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 the Council 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 including to the Governance Board. 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. As part of ICT's continual improvement processes, the ICT Security Manager will be producing quarterly cyber security highlight reports, informing Corporate Leadership Team (CLT) and Extended Corporate Leadership Team (ECLT) of the current threats being observed, including updates on strategy progress.

4.9.4 As a result of the preventative measures taken, there were no cyber security incidents that had a negative impact upon the Council in 2022/23.

4.9.5 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 A major records management piece of work across the Council is underway to move all electronic files into the MS365 Sharepoint environment. As part of this Shared Data Migration Project, data will be cleansed and only that which it is required to retain will be moved to the new filing structure. A programme has already taken place to move the personal drives of officers into the MS365 OneDrive environment. Once complete, these pieces of work will improve the ability to locate data for FOI/EIR requests and provide greater ability to specify access levels to data at a granular level. Training is being provided to those moving/disposing of data and the Council's Document Retention and Disposal Policy is being followed.

5.1.2 As mentioned above, arrangements for the handling of data protection support, Freedom of Information and Subject Access Requests changed in November 2022 as a result of the Business Support review and restructure. The centralised services for FOI, EIR and SAR requests will continue to develop throughout 2023/24 as officers new to the specialism develop in expertise and the anticipated greater flexibility to respond to peaks of work is delivered. Enhanced reporting is being 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.

5.1.3 The Good Governance Group has been replaced by a Governance Board. The Board will include within its remit driving improvement in information management. The data protection advisory service is now part of the Information Governance, Complaints and Resolution Hub. Policies and procedures have been updated to reflect the changes.

5.1.4 Through 2023/24 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.

5.1.5 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.

5.1.6 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.

5.1.7 ICT recently undertook a Public Service Network (PSN) security audit as part of their yearly accreditation. This was the first time, due to Covid, that the Council had undergone this audit. Issues highlighted in the report have been analysed, and any not being rectified as part of ICT's Tech Modernisation

Programme, were added to a plan to ensure they are resolved. This plan has been shared with the Cabinet Office.

6. Reasons for Decisions

6.1 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 frameworks.

7. Other Options

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

8. Financial Implications

8.1 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) and reducing the likelihood of costs associated with remedial actions following cyber-attack.

9. Legal Implications

9.1 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.

10. Carbon Impact

10. 1 None arising from this report.

11. Equalities

11.1 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.

12. Consultation

12.1 Internal

Appendices

None