Southend-on-Sea Borough Council

Report of the Chief Executive

to

Cabinet

on
18 September 2018

Report prepared by: John Williams, Director of Legal and Democratic Services and Senior Information Risk Owner (SIRO); Val Smith, Knowledge and Information Manager, Policy, Engagement and Communication

Information governance update and
Senior Information Risk Owner (SIRO) Annual Report 2017/18
Policy & Resources Scrutiny Committee
Cabinet Member: John Lamb
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 2017/18.

1.2 To report on opportunities and challenges in regard to information governance during 2018/19.

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 2017/18 be noted.

2.2 That the key actions taken during 2017/18, and the opportunities and challenges for 2018/19 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 the Council's Digital Strategy and Data

Protection Policies.

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 Director of 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 2017 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 – 2017-18

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 Director of Transformation and the Director of Digital Futures
- 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 PEC Team.

4.1.3 With regard to Cyber Security, the SIRO is supported by the Cyber Security Lead, (the Director of Digital Futures) and the Group Manager ICT. ICT monitor cyber security 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. ICT 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) assists the organisation in monitoring internal compliance, informing and advising on data protection obligations, providing advice and assistance on Data Protection Impact Assessments and acts 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 Corporate Information Governance Group (CIGG) but on occasions it will be the Corporate Management Team (on which the SIRO sits).

4.1.5 The DPO is assisted by the Data Protection and Freedom of Information Advisory Service located within Policy, Engagement and Communication. They provide the organisation with advice and training for these specialisms. They also manage Data Protection and Freedom of Information central records, monitor performance and compliance with legislation and lead on records management.

4.1.6 Leadership and governance of information management has been provided by the Corporate Information Governance Group (CIGG) who oversee implementation of the information management strategy and during 2017/18 acted as a project board for implementation of GDPR.

4.1.7 The CIGG is chaired by the Director of Transformation, with membership including the SIRO, the Council's two Privacy Officers, the Caldicot Guardian and the DPO.

4.1.8 During 2017/18 and until June 2018, a GDPR project group, chaired by the Head of Policy, Engagement & Communication and consisting of representatives across the Council, led on preparations for GDPR. The project group met regularly to progress a detailed GDPR project action plan. The group reported to the CIGG for approval of changes to policy and procedure.

4.1.9 To better serve the organisation, the Data Protection/Freedom of Information Co-ordinators Meetings have been reconstituted to become a Data Protection and Freedom of Information Community of Practice, led by the Knowledge and Information Manager. The COP continues to monitor performance but the focus on sharing good practice and providing training is being expanded, as is the role of its members in providing expert knowledge to their colleagues. The SIRO is a member of the COP.

4.1.10 The Council is a signatory to the Whole Essex Information Sharing Framework (WEISF) and the associated forum. This 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. All sharing agreements are hosted in a portal managed by Essex County Council.

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 2017/18 this comprised of formal class room training, induction training and SPARK e-learning module (which is also a gateway to permission being allowed to work remotely).

4.2.2 The Data Protection Officer has passed the examination for the Practitioner Certificate in Data Protection (awarded by PDP) and the Information Governance Advisor has attended a number of in-depth data protection courses in preparation for their role.

4.2.3 When examining data protection security incidents, the Data Protection Advisory Service routinely consider resultant training needs, advising attendance at one of the training options or bespoke training as required.

4.2.4 In addition to the standard training options, a series of face to face training events designed to raise awareness of GDPR were delivered, tailored to different audiences. An awareness session for Members was also held. These sessions reached 417 delegates over 13 sessions. For those staff not requiring specialist training, desk based training was provided.

4.2.5 During 2017/18 the Council's traded services for schools included assistance from the GDPR Project Manager with preparation for GDPR, including policies and procedures and in person discussions. As from 25 May 2018 schools are required to have their own Data Protection Officer, this service has now ended. An on-line Schools Data Protection Officer Community of Practice has been established on the SBC School Learning Network to facilitate Schools DPOs in assisting each other.

4.2.6 In preparation for GDPR, a series of messages were provided to staff alerting them to the new legislation. These included blogs from the Chief Executive and Data Protection Officer, posters emphasising the value of personal data, 'In the Loop' content and animated videos.

4.2.7 In addition to the above, throughout 2017/18 ICT have delivered training and awareness sessions specifically relating to cyber security. Regular cyber security messages are issued by ICT to staff.

4.2.8 The Workforce Strategy team in the Department for People provided e-learning training materials for the use of external Adult Social Care providers to assist them in their duty to correctly process the data of their staff and residents. School nurses receive additional training to meet NHS requirements.

4.2.9 As a result of all the above, staff awareness of data protection requirements and associated organisational processes has been raised. This is a welcome outcome, however it is generating a considerable amount of associated work for the Data Protection Advisory Service and this is expected to continue during 2018/19 while the new processes bed in.

4.2.10 As can be seen from the above, there are a number of strands to the data protection training being provided. During 2018/19 a revised approach is being devised. This will be based on e-learning of varying levels of complexity dependent on need, bite-sized learning to promote general awareness and face to face training for those who need to understand the organisational context or where there is an identified specialist audience. The current SPARK e-learning module will be replaced.

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 DPA 1998 has been repealed and is superseded by the DPA 2018. The provisions of the GDPR will remain in effect when the UK leaves the EU as it will be adopted into UK law. The GDPR and DPA 2018 must be read side by side when considering the application of data protection legislation.

4.3.6 During 2017/18 the GDPR Project Group led on the preparations of the Council for GDPR and the DPA 2018. The Group worked to a detailed project plan which was independently externally audited by data protection specialists ‘Act Now’ to ensure it incorporated all necessary steps for successful transition to the new legislation.

4.3.7 The breadth of knowledge of the organisation and the insight which the team provided proved invaluable and, while the project has now finished, a GDPR Group comprised of former project group members will continue for at least a further six months to support the bedding in of new processes.

4.3.8 Preparation for the new legislation provided an opportunity for the Council to review and enhance its systems and processes for managing information, how it uses data and other information and ensuring personal data is kept secure.

4.3.9 During the project, the Council’s data protection policies and procedures were reviewed and revised to ensure compliance with the new requirements. Significant among these were revised processes for enhanced data subject rights, data security incidents and data protection by design and default.

4.3.10 A further significant effect of the new legislation is that the Council can seldom rely on the previously commonly used ‘consent’ or ‘legitimate interests’ as a basis for processing personal data. An alternative basis from those available has to be identified by services and this is requiring some adjustment in thinking.

4.3.11 Where the Council is a Data Controller, contracts and Information Sharing Agreements have been being reviewed on a risk basis and are being varied where required. Similarly, where the Council is a Data Processor, the relevant contractor is requiring the Council's acceptance of contract variations. Procurement and the Data Protection Advisory Service will continue to work closely with contract managers during 2018/19.

4.3.12 Although processes have been developed and published, it will take time for them to bed in and become business as usual. In particular, the impact on volumes of work of the newly introduced data subject rights and of the withdrawal of the fee for subject access requests will only become apparent over time.

4.4 Information Governance Toolkit

4.4.1 The Information Governance Toolkit (IG Toolkit) is a Department of Health (DH) policy delivery vehicle which draws together the legal rules and central guidance set out by DH policy and presents them in a single standard as a set of Information Governance requirements.

4.4.2 This independently audited self-assessment tool enables the Council to demonstrate to DH that it can be trusted to maintain the confidentiality and security of personal information, in particular Public Health and Adult Social Care personal records.

4.4.3 The 2017/18 IG Toolkit was successfully completed with the Council achieving a score of 95%. Out of 28 requirements, the Council achieved level 3, the highest possible level, in 24 requirements and a level 2 in the remaining 4.

4.4.4 For 2018/19 the toolkit has been rebranded as the Data Security and Protection Toolkit and will have an increased focus on cyber security. Work is underway in the Data Protection Advisory Service to identify the new requirements and in particular to liaise with colleagues in ICT and the Emergency Planning and Business Continuity team to ensure that the Council will be compliant.

4.4.5 These actions, the revised structure and resourcing for emergency planning and business continuity and the ICT Disaster Recovery Plan, will support the GDPR requirement for organisations to ensure they have 'the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident'.

4.5 Freedom of Information

4.5.1 Under Freedom of Information legislation, individuals are entitled to ask the Council for a copy of information it holds. This is known as a Freedom of Information request (FOI).

4.5.2 1238 FOI requests were received in 2017/18, compared to 1185 in 2016/17. To ensure consistency and compliance the FOI function is managed corporately within the Policy, Engagement and Communication (PEC) team. 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 PEC.

4.5.3 In 2017/18 the Council replied to 1192 requests, 75.08% within the required 20 working days. This compares to 1160 replied to in the previous year with 84.22% compliance. The Information Commissioner has indicated that their expectation is in excess of 90% compliance and ways of improving the Council's performance are being considered by PEC and the Data Protection and Freedom of Information Community of Practice.

4.5.4 The Council's Freedom of Information Publication Scheme has been updated to provide regularly requested information in a more accessible and up to date way. Further work is being undertaken to promote an open and transparent approach to providing information to residents, and others, which, in addition to enabling them to be better informed should also help to reduce the number (and/or complexity) of FOI requests that would otherwise be processed.

4.6 Subject Access Requests

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

4.6.2 There have been 64 SARs processed in 2017/18 an increase from 55 in the previous year. These are requests from customers for copies of their personal data held by the Council. The Council replied to 56.25% of these requests within the 40 calendar day target. 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 In 2018/19 additional resource has been provided for the Department for People, who have the majority of SAR requests, to increase the speed with which requests are processed. Early indications are that an improvement is already being demonstrated.

4.6.4 It is not yet known whether the removal of the former £10 charge for a SAR will result in an increased number of applications.

4.7 Requests for Data Sharing

4.7.1 In 2017/18 a total of 918 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 PEC team.

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 continue 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 41 data security incident investigations were undertaken in 2017/18 from which 20 breaches were identified. Recommendations were made to the SIRO on the significant cases.

4.8.2 In 2017/18 no data breaches required notification to the Information Commissioner. The threshold for reporting data security breaches to the ICO has however changed under GDPR and the effect of this on the Council's reporting to the ICO during 2018/19 is yet to be determined.

4.8.3 The data protection training carried out in 2017/18 has raised awareness within the organisation of the need to formally report data security incidents and early indications are that this is likely to result 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 training 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.

4.9.3 The Council's Information Asset Register has been digitised during 2017/18. During 2018/19 it will be systematically reviewed and updated as new assets are introduced. The longer term aspiration is for all data protection records to be electronically cross-referenced to the relevant information asset, allowing the Council improved assurance regarding data protection compliance.

4.10 Information Security (including Cyber Security)

4.10.1 The 'Cyber Essentials' scheme is a government backed, industry-supported scheme to help organisations protect themselves against common online threats. ICT have been using its principles to inform the Council's approach to cyber security and will continue to do so in 2018/19. The PSN Code of Practice is being used similarly. As a result older technology, such as Lagan and CareFirst, has been retired and is being decommissioned.

4.10.2 Following the cyber security internal audit in 2016, the Council's security posture with external consultants has been reviewed and changes regarding processes and software to manage and contain RansomeWare have been made. A further internal audit will be undertaken during 2018/19 where the current position will be assessed.

4.10.3 In 2017/18, in accordance with national guidance, specific procedures were put in place to guard against the possibility of state-sponsored attacks on election processes. This risk will continue to be assessed during 2018/19.

4.10.4 During 2018/19, with the Essex On-Line Partnership, the Council will contribute to the development of the Local Government Association's cyber security stocktake questionnaire which will ultimately be rolled out for organisations to use to assess their cyber security position.

4.10.5 In 2018/19 ICT will move the organisation from its current secure e-mail platform, GCSX, to DMARC systems. This will provide improved security for confidential or sensitive e-mailed information.

4.10.6 Scoping for a Data Warehouse for the Borough continues. Partners across Essex are assisting by sharing their experience of creating such a facility.

4.10.7 The movement of on-premises IT systems to the more secure environment of the new server room was progressed during 2017/18 and will continue during 2018/19.

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 the coming months will, as described above, be to consolidate and capitalise on the progress already achieved during the preparations for GDPR.

5.1.2 This will put the Council in a sound position to fulfil its ambition of using data and information more effectively and complement other key areas of work including its ambitions for Southend 2050, Transformation and Channel Shift, Digital Strategy and Infrastructure, Big Data and Open Data.

7 Corporate Implications

7.1 Contribution to the Council's vision and Corporate Priorities.

Sound information management and the protection of personal data contribute to all the Council's aims and corporate priorities.

7.2 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).

7.3 **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.

7.4 **People Implications**

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

7.5 **Property Implications**

None

7.6 **Consultation**

Internal

7.7 **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.

7.8 **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.

7.9 **Value for Money** - None

7.10 **Community Safety Implications** - None

7.11 **Environmental Impact** - None

8 **Background Papers** - None

9 **Appendices** - None