Southend-on-Sea Borough Council

Report of the Chief Executive

to

Cabinet

on
7 November 2017

Report prepared by: John Williams, Director of Legal and Democratic Services and Senior Information Risk Owner (SIRO); Tim MacGregor, Team Leader, Policy & Information Management

---

Information governance update and
Senior Information Risk Owner (SIRO) Annual Report 2016/17
Policy & Resources Scrutiny Committee
Executive Councillor: Councillor Moring
A Part 1 Public Agenda Item

---

1. Purpose of Report

1.1 To provide an update on the Council's approach to information governance and management.
1.2 To comply with the requirement for the SIRO to provide an annual report.
1.3 To report on action being taken to prepare for impending new legislation relating to data protection and information management.

2. Recommendations

2.1 That the SIRO's report on Information Governance for 2016/17 be noted.

2.2 To note the introduction of the General Data Protection Regulation (GDPR) from 25 May 2018 and publication of the Data Protection Bill along with the related implications of these measures for the Council.

2.3 Note the action being taken by the Council to prepare for the GDPR and Data Protection Bill.

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, the context and challenges faced by the Council (including the new requirements of the GDPR) along with 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 Policy.

3.2 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. Since 1 October 2016, the SIRO for the Council has been the Director of Legal and Democratic Services.

3.3 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 2016 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 Data Protection Act 1998.

4.0 SIRO Annual Report – 2016-17

4.1 General Data Protection Regulation and Data Protection Bill

4.2 A new European Union data protection framework was adopted in April 2016 and takes the form of the 'General Data Protection Regulation'. The GDPR will become effective from 25 May 2018 and will supersede the Data Protection Act 1998. The Government has confirmed that the UK's decision to leave the EU will not change this position. This is because the GDPR also applies to organisations outside the EU offering goods or services to EU citizens and because the Government supports the principles and content of the regulation.

4.3 The GDPR is designed to create a uniform approach to data protection across Europe, one that takes account of developments in ICT and media and which empowers citizens and enhances economic growth by removing barriers to data flows.

4.4 To enable compliance with the GDPR the Government introduced (in September 2017) a Data Protection Bill, which, the Government states, will:

- Make UK data protection laws 'fit for the digital age' in which an ever increasing amount of data is being processed.
- Empower people to take control of their data.
- Support UK businesses and organisations through the change.
- Ensure that the UK is prepared for the future after it has left the EU.

4.5 Key measures of the GDPR:

Key measures that will impact on the Council include:

- Significantly higher maximum penalties for serious data breaches – up to £17m or 4% of turnover (up from the current maximum of £500,000);

- Enhanced rights for individuals, including:

- The right to be informed – the GDPR sets out the information that individuals should supply and when individuals should be informed;
- The right to erasure (the 'right to be forgotten') - individuals will have a right to approach the Council to erase/delete their data where there is no compelling reason for its continued processing;
- The right to data portability - an individual may request that the Council transfer data it holds on them to other organisations;
- The right to object – individuals have the right to object to the processing of their data under specific circumstances.

- Higher standards for ensuring consent from individuals for the use of their data, including the need for explicit consent. ICO guidance suggests public bodies should avoid using consent as a basis for processing where other means are available.

- The Council (and all public bodies) will no longer be able to rely on citing 'legitimate interests' for processing data, and will have to rely on other conditions such as statutory requirements instead.

- A requirement by the Council to report serious data breaches within 72 hours.

- Abolition of fees for most Subject Access Requests (the Council currently charges £10) and a requirement to process within a month rather than 40 days;

- A mandated requirement for Data Protection Impact Assessments (Privacy Impact Assessments) to include data protection controls at the design stage of new projects involving the processing of personal data. In addition to projects, DPIAs will be required for new contracts and significant changes in processes.

- A Data Protection Officer (DPO) must be appointed, who is required to be independent of, but directly link with the senior management structure. The Council must ensure the DPO is properly resourced to perform their duties;

- A 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';

- A requirement for data controllers to be able to *demonstrate* compliance with the principles of GDPR as opposed to retrospectively giving evidence when asked.

- The Information Commissioners Office (ICO) will have powers to audit councils, triggered by public complaints from the public;

4.6 Data Protection Bill

The Government has stated that the *Data Protection Bill* will 'implement the GDPR standards across all general data processing', and will:

- Provide clarity on the definitions used in the GDPR in the UK context.
- Ensure that sensitive health, social care and education data can continue to be processed to ensure continued confidentiality in health and safeguarding situations can be maintained.
- Provide appropriate restrictions to rights to access and delete data to allow certain processing currently undertaken to continue where there is a strong public policy justification, including for national security purposes.
- Expand the definition of 'personal data' to include IP addresses, internet cookies and DNA.
- Set the age from which parental consent is not needed to process data online at 13.

4.7 Cyber Security

In line with the Data Protection Bill, the Department for Digital, Culture, Media and Sport has undertaken a consultation on implementing the EU Network Information Systems (NIS) Directive. The Directive (which must come into effect by May 2018) aims to achieve a high common level of network and information systems security across EU states by requiring the introduction of security measures and incident reporting obligations for digital service provides.

The Directive could similarly see organisations face fines of up to £17m, or 4% of global turnover if they do not make their information safe, secure and resilient against cyber-attacks. Once implemented the NIS Directive will form an important part of the Government's five-year £1.9 billion National Cyber Security Strategy.

4.8 Key Implications for the Council:

- The new GDPR and legislation provide an opportunity for the Council to review and enhance its systems and processes for managing information that will enable it to exploit, more effectively, its use of data and other information and ensure personal data is secure.

- A significant growth in workload in preparing for the GDPR, in maintaining new processes, in responding to enhanced individual rights, and greater public awareness of these rights, for example, there is an anticipated growth in Subject Access Requests.

- The Council will need to embed a 'data protection by design culture' so that consideration of the use of information and data protection is built into processes from start to finish, of projects, service re-design and contract letting and management.

- There will be a need to raise awareness of all staff and Members of the implications of the new requirements, but particularly those involved in the processing of personal data. This will require implementation of a comprehensive communication and training strategy and will need to encompass arms-length companies (South Essex Homes and Southend Care), schools, agency and temporary staff;

- The Council will need to ensure it has comprehensive and complete records to show where Council's data is stored, why it is held, how it is being used and how it complies with GDPR requirements. This can be achieved by updating the Council's Information Asset Register;

- A need to review consent practices, including existing consents and refresh consents if they do not meet the GDPR standard.

- GDPR applies to 'data controllers' as well as 'data processors' and so places greater emphasis on obligations placed on Council contractors, in relation to the protection of data they process on behalf of the Council. Contracts and Information Sharing Agreements will need to be reviewed on a risk basis to ensure they remain compliant with GDPR, and varied or terminated if they do not. A register of contracts involving data sharing, and Information Sharing Agreements with third parties (including SEH, Southend Care and NHS bodies) should be maintained.

- The Council will need to review Data Protection Impact Assessment processes before undertaking projects potentially involving data processing.

5. Report on Activities since April 2016

5.1 Key actions to enhance the Council's approach to information management and anticipate GDPR include:-

- As outlined in paragraph 3.1, the **Council's Information Management Strategy** was agreed in June 2016. The strategy set out a vision for how the Council manages information:

  'To create a culture that promotes the creative and innovative use of information to empower residents, enhance efficiency and generate fresh approaches for the Council to achieve its aims. The Council will: ensure personal data is held securely; ensure information is disseminated effectively; be transparent and enabling in its handling of information and operate within the necessary legal framework'.

  It also agreed 6 principles that Council officers and Members should adhere to:

  i) Hold personal data and information securely and safely;
  ii) Adopt a proportionate, risk based approach to security and information governance, ensuring that controls do not provide a barrier to innovation;

iii) Promote and apply a transparent approach to the release and provision of information and data, publishing information in a way that is easy to find and in a format that is easy to re-use;
iv) Support a collaborative approach to the creation, use and sharing of information, both internally and externally, where this is appropriate and in the interests of local communities and service users;
v) Ensure that data is accurate; valid; reliable; timely; relevant and complete and
vi) Ensure information is stored in a way that it can be found, used and re-used and is available in the event of an interruption to service.

- Since then the related actions have been taken forward, by a corporate information management group and designated officers.

- Following the senior management restructure in Autumn 2016 (which saw the deletion of the post of the then SIRO, the Corporate Director for Corporate Services) a reconfiguration of the **leadership and governance arrangements** for information management has been undertaken to:

  - Constitute a **Corporate Information Governance Group (CIGG)** to oversee implementation of the information management strategy and act as project board for implementation of GDPR. The board is chaired by the Director of Transformation, with membership including the SIRO in attendance, the Council's two Privacy Officers and Caldicot Guardian.

  - Appoint a replacement Privacy Officer (the new SIRO was previously a designated 'privacy officer').

- A revised **Digital Strategy (2017-20)** was approved by Cabinet in June 2017. The strategy outlines a vision to utilise technology to support the Council's aims and priorities, requires the Council to adopt a 'digital by default' ethos in its interactions with the public, internal processes and working with partners and move Southend into becoming a leading SMART city.

  The strategy includes an action to establish an 'intelligence hub' to collect data from a range of technology sources, providing a more holistic, integrated and instant means of shaping services and places to people's needs. To progress this approach, 'proof of concept' pilots are to be undertaken in the areas of community safety; traffic flow and parking management; health & wellbeing (assistive living); environment monitoring and management and energy.

- The **Policy, Engagement and Communication Group (PEC) was restructured** in January 2017 to introduce a more robust structure to deal with information management and complaints, including preparing for GDPR.

- A permanent **designated Data Protection Officer,** (Val Smith - Knowledge and Information Manager, located in the PEC Team) was appointed, alongside a fixed term project manager for GDPR, in April 2017.

- A **GDPR project group** has been established, chaired by the Group Manager for PEC and consisting of representatives across the Council. The project group is meeting regularly to progress a detailed GDPR project action plan up to May 2018 and beyond. It reports to the Corporate Information Governance Group.

- The requirements of version 14 of the **Information Governance Toolkit** were successfully completed with the Council achieving 95% compliance. This self-assessment tool enables the Council to process Public Health and Adult Social Care personal records. Out of 28 requirements, the Council achieved level 3, the highest possible level, in 24 requirements and a level 2 in the remaining 4.

- The Council's Privacy Impact Assessment (PIA) template has been further developed to meet the requirements of GDPR. The PIA (to be renamed Data Protection Impact Assessment) is a structured assessment of potential impact on data subjects' privacy of a new 'system'. It forms part of the overall risk assessment of a project or defined piece of work. The PIA process includes a flow chart to ensure that all contract managers take data governance into account when letting and managing contracts. Since the template was launched in Nov 2015, 36 PIAs have been completed.

- As a signatory to the Whole Essex Information Sharing Framework (WEISF) the Council is able to share 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.

- The changes to senior management structures and departmental arrangements (from Autumn 2016) saw the incorporation of the public health function into the People Department, including the alignment of information/data specialists, helping to promote a more holistic approach to data analysis.

- Regular training in data protection and information management sessions have resulted in improved staff awareness of information governance requirements and associated organisational processes.

- Key actions from the Information Commissioner's Office consensual audit undertaken in 2012/13 are continually reviewed.

5.2 Leadership and Governance

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.

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 (all Group Managers)
- The Council's Data Protection Officer – Knowledge and Information Manager in the PEC Team.

5.3 Training and awareness

Data Protection training continues to feature as a key part of ensuring staff are aware of their responsibilities. In 2016/2017, 15 sessions were undertaken, including corporate awareness sessions, tailor made sessions following a breach/potential breach, corporate induction. One training session was held for a school.

Staff continue to complete the mandatory Data Protection e-learning tool with 65.8% of staff having completed this training. Successful completion of this is also a requirement for staff to work remotely.

Messages promoting good data protection practice, handling a data breach/complaint, and a message from the Caldicott Guardian on the need for security of personal data in transit were included in the 'In the Loop' staff newsletter. Messages relating to ICT security and ensuring vigilance on visitors to council offices have been circulated regularly to all council staff via 'everyone emails'.

5.4 Freedom of Information (FoI)

1185 FoI requests were received in 2016/17, compared to 1101 in 2015/2016, 1108 in 2014/15 and 983 in 2013/14. The FOI function sits in the Policy, Engagement and Communication Team. The Council replied to 84.22% requests within 20 working days. Most of these requests, at 48%, were received from the public, 31% from other organisations and 11% from the media and 10% from other sources (including researchers, MPs, councillors).

The Council's 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 will also help to reduce the number (and/or complexity) of FOI requests that are processed.

5.5 Data Protection

There have been 55 Subject Access Requests (SARs) processed in 2016/2017, These are requests from customers for copies of their personal data held by the Council. The Council replied to 66% of these requests within the 40 calendar days target. The fact that 33% of SARs took longer than 40 days is a reflection of the significant time involved in responding to many of these requests particularly where these have been historic child care requests.

In 2016/17 a total of 973 ‘section 29/35’ requests were received. These are requests, mostly received from the Police, for third party information. These requests were received through Legal and Democratic Services, Revenues and Benefits, Counter Fraud and Investigation and the PEC teams.

Work to transfer all ‘section 29/35’ requests onto Covalent (the Council’s performance monitoring system) has been completed. The single gateway approach encourages consistency in recording; increases efficiency in monitoring the requests through automatic triggers; enables the maintenance of audit trails and facilitates the production of timely and accurate reports.

Regular communication, and training continues to raise awareness of the importance of data protection amongst staff. This has led to an increase over time in the reporting of data breaches, which ultimately helps with continual improvement in this area.

26 breach incidents were reported in 2016/17 (28 in both 2015/16 and 2014/15). Investigations were undertaken and recommendations made to the SIRO on the significant cases. To mitigate further incidents, evaluations were carried out to ensure recommendations were implemented.

As a part of the process, one data protection complaint was investigated by the ICO in 2016 with an explanation of mitigation and corrective action. The ICO took no further action.

5.6 Records Management

With increasing public access to Council records, it is important that necessary documents are retained and that records are disposed 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. This Policy is currently being updated to reflect GDPR requirements.

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. It informs where the Council’s electronically held and hard copies of data are held. Work is underway to update the register to ensure it is GDPR compliant and meets the needs of service areas.

Data Protection training sessions now include aspects of records management and the Information Asset Register helping to further increase awareness on the secure disposal and archiving of records.

5.7 Information Security

The Council has a comprehensive Information Security Framework to support the current and evolving information security requirements**.**

A cyber security action plan, setting out the activities required to be delivered over the coming year to gain the accreditation to the Government-backed 'Cyber Essentials' scheme was approved by the Council's Digital Board in March 2017,

An internal audit of Council cyber security arrangements was undertaken in 2016. It found that 'The foundations are in place for the management of cyber security across the Council' and that the' technical documentation setting out how to deal with cyber security is in line with best practice and processes are maturing and that operational issues around Data Protection are handled to a satisfactory level'. The audit also found that Cyber security principles are embedded within the extensive policy set and wider IT documentation. Security plans are in place.

However, further work was identified as required to move the Council towards higher levels of assurance. This includes: a formalising roles; clarifying accountabilities and responsibilities and updating policies in line with the latest government guidance. In addition, it was noted that areas such as information handling and information asset registers, will increase the overall assurance over cyber security across the Council.

It was noted that the 'creation of a strategy, with reference to the National Cyber Security Strategy (November 2016), will help the Council align its activities with government's strategy'. The Council's IT Corporate Information Security Policy, Acceptable Use Policy and Using Email and Digital Communications have been or are currently being refreshed by the Essex Online Learning Partnership.

6 Strategic Direction - Future Programme of Work

6.1 A major focus for the Council in relation to information management in the coming months will, therefore, be to ensure the Council is compliant with the GDPR, Data Protection Bill and other legislative requirements. In addition to the measures set out above, the Council has undertaken a gap analysis of its readiness for GDPR which will inform the GDPR Project and related action plan. A further audit will be undertaken in January 2018, to assess progress on the action plan.

6.2 This activity will put the Council in a better position to fulfil its ambition of using data and information more effectively and complement other key areas of work including:

- **Channel shift** – the continuing move of customers away from face to face and phone contact to 'self-serve' primarily through the My Southend portal, so that by 2019/20, 90% of interactions with the council will be online.

- **Digital infrastructure** – introduction of new digital infrastructure across the borough with pure fibre connection providing super-fast connectivity for council building, schools, businesses and homes. The Council's Digital Strategy outlines how improved connectivity, offering Gigabit speed, will help to better drive council services, reduce costs, and provide opportunities 'for energy saving, carbon reduction, citizen focus, innovation and sustainable growth' for its residents and

businesses.

- **Big Data** – the more effective and creative use of what is often referred to as an 'untapped goldmine' of information, matching different data sources to identify better outcomes for residents.

- **Open Data –** making more Council information and data freely available, in re-usable formats, should reduce the number of FoI requests, with a view to reuse and redistribution. Such information would need to adhere to data protection requirements and making it available would require careful consideration of risks around data quality, potential for mis-use, along with any commercial and financial sensitivities. However, providing data for others, including academics, charities and public, may provide some interesting findings and new policy options that may not otherwise have been considered.

Further information and briefings will be provided for members and staff on a regular basis as statutory requirements are clarified and further guidance issued by the Government and ICO in preparation for implementation of GDPR.

7 Corporate Implications

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

Contributes 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 for security breaches).

7.3 Legal Implications

Information management and Data Protection are subject to a range of legislation, including:

Human Rights Act 1998
Data Protection Act 1998
Environmental Information Regulations 2004
Freedom of Information Act 2000
Computer Misuse Act 1990
The Access to Health records
Civil Contingencies Act 2004
Crime and Disorder Act 1998
Children Act 2004
Health and Social Care Act 2012
Social Security Administration Act 1992 (in respect of benefits data)

The GDPR and Data Protection Bill will replace the Data Protection Act and

introduce a range of new requirements on local authorities, as set out in the 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**

The Council collects a range of information to help it meet the needs of its customers and staff, including, where relevant, information on the "protected characteristics‟ as defined in the Equality Act 2010 (age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race & national origin, religion and belief, sex, sexual orientation). In line with the Act the Council, each year, publishes a profile of its customers (along with how they rate services) and its workforce, and who share protected characteristics. All information is collected and maintained in line with the Data Protection Act, for example, to ensure it is anonymous.

7.8 **Risk Assessment**

Non-compliance with the law would adversely affect the Council's reputation in the community and reduce public trust and could lead to "incidents‟ with 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