Southend-on-Sea Borough Council

Agenda Item No.

Report of the Corporate Director for Corporate Services

to

Cabinet

on

20th September 2016

Report prepared by: Sally Holland, Corporate Director of Corporate Services and Indi Viknaraja – Data Governance Advisor
Policy, Engagement & Communication (PEC)

Information Governance
Senior Information Risk Owner (SIRO) Annual Report 2015/16
Policy & Resources Scrutiny Committee
Executive Councillor: Councillor Moring

---

1. Purpose of Report

The Senior Information Risk Owner "(SIRO)" is required to produce an annual report to Cabinet on:

a. assurances of progress and developments in Information Governance in 2015/16; and
b. the strategic direction for Information Governance work for 2016/17.

2. Recommendation

To note the SIRO's Report on Information Governance in 2015/16 and the proposed work for 2016/17.

3. Background

3.1 The SIRO takes overall responsibility of the Council's information management framework; acts as the champion for information risk within the Council and ensures an Annual SIRO Report on Information Governance is presented to Members. The SIRO for the Council is Sally Holland, the Corporate Director for Corporate Services although from 1st October 2016, it will be John Williams, Head of Legal and Democratic Services.

3.2 This Annual Report provides Members with an overview of the Information Governance work carried out in 2015/16 and demonstrates that personal data is held securely; information is disseminated effectively and enables the handling of information within the necessary legal framework, and particularly the Data Protection Act 1998. This report also outlines proposed action in 2016/17.

4. Report on 2015/16 Activities

4.1 Key Actions in 2015/16

- The requirements of Version 13 of the Information Governance Toolkit were successfully completed with the Council achieving 86%. 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 17 requirements and a level 2 in the remaining 11.
- A Privacy Impact Assessment (PIA) template has been commissioned through the Business Processes/Project Management Guidance. A PIA 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. The template was launched in Nov 2015 by the SIRO and to date, 19 assessments have been completed.
- A procurement flow chart to include Data Protection and PIA requirements has been produced to ensure that all contract managers take data governance into account when letting contracts.
- 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.
- Obtaining pioneer status in creating new models for integrating NHS and social care services has helped to focus on tackling issues of information sharing between partner organisations. It enables single, comprehensive datasets for the purpose of risk stratification and commissioning, all aligned to single packages of care to encapsulate patient/client needs.
- The Department of People has established integrated data and commissioning teams. This facilitates the combination of different systems relating to children and adults and offers a more holistic analysis of matched data in the Council. To support this function, and adequately address the requirements under the Data Protection Act, due consideration has been given to the purpose for which personal data is collected, fair processing notices and consent, to ensure that all processing is fair and lawful.
- 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 (ICO's) consensual audit undertaken in 2012/13 are continually reviewed. These include the following:
    - The Overarching Information Management Strategy has been updated to reflect changes to governance arrangements in the Council.
    - In line with the Offsite Storage Policy, data transfer sheets are kept by service areas and the Customer Service Team.

4.2 **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 also provides the Annual SIRO Report in regard to information management and risk.

The SIRO's role is supported by:

- The Chief Privacy Officers (Data Controllers) - the Head of Legal and Democratic Services and Head of Customer Services
- The Caldicott Guardian - the Head of Children's Services
- The Information Asset Owners (Group Managers)
- The Data Governance Advisor

4.3 Training and awareness

Data Protection training continues to feature as a part of the corporate, team and induction training programmes. In 2015/2016, twenty seven training sessions were carried out. This includes 4 training sessions at schools, and the remaining provided within the Council's regular training programme, Induction, and the tailor made sessions after a breach/potential breach.

Staff continue to complete the mandatory Data Protection e-learning tool (90% of staff have completed this training). Successful completion of this is also a prerequisite for staff to work remotely.

4.4 Freedom of Information

A total of 1101 requests were received in 2015/2016, compared to 1108 in 2014/15. The FOI function sits within the Policy, Engagement and Communication Team. The Council replied to 85.89% requests within 20 working days. The majority of these requests, at 48.54%, were received from the public, 35.04% from other organisations and 10.49% from the media.

The Council's Publication Scheme has been updated to provide regularly requested information in a more accessible and up to date way. This also helps to reduce the number of FOI requests that are processed.

4.5 Data Protection

There have been 117 Subject Access Requests (SARs) processed in 2015/2016, compared to 151 processed in 2014/2015. These are requests from customers for copies of their personal data held by the Council. The Council replied to 68.12% of these requests within the 40 calendar days. The fact that 31% 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 2015/16 a total of 1149 section 29 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 requests onto Covalent (the Council's Performance Monitoring system) is underway. 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.

The Council's Communications Strategy and regular training continues to raise awareness of the importance of Data Protection amongst staff. This has led to an increase in the reporting of data incidents, which ultimately helps with the continual improvement.

A total of 28 incidents were reported for 2015/16. 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 incident where envelopes were mis addressed was "self-reported" to the ICO in 2015 with an explanation of mitigation. The ICO took no further action.

4.6 Records Management

With increasing public access to our records, it is important that necessary documents are retained and that disposal of records happens as part of a managed process and is adequately documented. Therefore Directorates 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 support the Council's Document Retention and Disposal Policy. This Policy is currently being updated.

The Council has an Information Asset Register. This is a mechanism for understanding and managing the Council's information assets and the risks to them. It is a register which informs where the Council's electronically held and hard copies of data are held. Work is underway to update the register and to make it available on the Council's intranet site.

Data Protection training sessions now include aspects of Records Management and the Information Asset Register. These help to further increase awareness on the secure disposal and archiving of records.

4.7 Information Security

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

The Council's IT Corporate Information Security Policy, Acceptable Use Policy and Using Email and Digital Communications are currently being refreshed by the Essex Online Learning Partnership.

An ICT Security Audit has been carried out to ensure that the Council has appropriate technical and organisational measures to prevent unauthorised and unlawful processing of personal data. The report from the Audit is expected by end of September 2016.

5 Strategic Direction - Future Programme of Work - 2015/16

Data Protection

5.1 While the EU's General Data Protection Regulation (GDPR) was finalised, and is scheduled to come into force on 25th May 2018, the uncertainty of the outcome of UK negotiations on the terms of it's exit from the EU brings into question whether or for how long the Regulation will directly apply in the UK.

A statement from the Information Commissioner's Office (ICO) confirmed that the Data Protection Act "remains the law of the land" at the moment. It said that UK Data Protection reforms are "necessary" and that the Data Protection framework in the UK would need to accord to the standards outlined in the GDPR if the UK wishes to "trade with the [EU] single market on equal terms" in the event that the Regulation does not "directly apply to the UK".

"If the UK is not part of the EU, then upcoming EU reforms to Data Protection law would not directly apply to the UK. But if the UK wants to trade with the single market on equal terms we would have to prove 'adequacy' - in other words UK Data Protection standards would have to be equivalent to the EU's General Data Protection Regulation framework starting in 2018."

Developments on this will be monitored. Any outcome will pose significant challenges to the Council, and will be addressed accordingly.

5.2 **General**

Further to team restructures and continued organisational changes, 2015/16 proved to be a very challenging year for the Council. In 2015/16 the Policy, Engagement and Communication team will continue to work across all areas of the Council to meet the requirements of governance legislation. In particular, it will work to meet the requirements of the Local Government on data handling and sharing, the use of big and open data and cyber security.

6 Corporate Implications

6.1 Contribution to the Council's Vision and Corporate Priorities.

Excellent – Deliver targeted services that meet the identified needs of our community.

6.2 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).

6.3 **Legal Implications**

Legal requirements must be complied with to ensure an individual's rights are respected. Inadvertent disclosure of data could leave the Council open to legal claims and fines. The collection, use and disclosure of personal information are governed by a number of different areas of law. The main pieces of legislation governing an individual's rights are:

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

6.4 **People Implications**

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

6.5 **Property Implications**

None

6.6 **Consultation**

Internal

6.7 **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, 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.

6.8 **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.

6.9 **Value for Money**

No issues

6.10 **Community Safety Implications**

None

6.11 **Environmental Impact**

None

7 Background Papers

None

8 Appendices

None