Southend-on-Sea Borough Council

Report of the Corporate Director for Corporate Services
to
Cabinet
on
10th November 2015

Report prepared by: Indi Viknaraja – Data Governance Advisor
Policy, Engagement & Communication

Information Governance
Senior Information Risk Owner (SIRO) Annual Report
Policy & Resources Scrutiny Committee
Executive Councillor: Councillor Woodley

---

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 achievements in 2014/15; and
b. the strategic direction for Information Governance work for 2015/16.

2. Recommendations

2.1 To note the SIRO'S Report on Information Governance in 2014/15 and the proposed work for 2015/16.

3. Background

3.1 The Council is required to appoint a SIRO to take overall ownership of the Council's Information Management Strategy; act as advocate for information risk for the Council and provide an annual SIRO report on Information Governance to Members. The SIRO for the Council is Sally Holland, the Corporate Director for Corporate Services and this report has been prepared on her behalf.

3.2 This annual report provides Members with an overview of Information Governance work carried out in 2014/15 and to demonstrate that personal data is held, maintained and shared in accordance with the law particularly the Data Protection Act 1998. This report also details proposed action in 2015/16.

4. Report on 2014/15 Activities

4.1 Key Actions in 2014/15

- The Council signed up to the Whole Essex Information Sharing Framework (WEISF) to formalise the sharing of information with Essex wide partners. As a partner to WEISF, this Council has agreed to actively promote the sharing of data whilst protecting service users' confidentiality.
- Key actions from the Information Commissioner's Office (ICO's) consensual audit undertaken in 2012 are continually addressed. These include the following:

    - Regular review of the Information Asset Register which maintains a list of all physical and electronic storage of personal data.
    - The Overarching Information Management Strategy is appropriately updated to reflect changes to governance arrangements in the Council.
    - All s29 requests (third party data requests) are processed in line with the procedures outlined in 'How to Process a Section 29 Request.

- The Care Act, which came into force in April 2015, places a duty on the Council to carry out its care and support functions with the aim of integrating services with those provided by the NHS and other health related services. To support this duty, 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.
- Southend was one of the 14 pioneers to participate in the Integrated Care Programme. All steps were taken to comply with the obligations of the Data Protection Act. Appropriate fair processing notices, with 'opt out' facilities were used to ensure the fair collection of personal data and, where applicable, this Council actively sought consent from its residents.
- As the Council processes Public Health and Adult Social Care related personal data, it has to carry out an annual assessment against the Department of Health's Information Governance policies and standards, to ensure that personal data is handled correctly and is protected according to the Data Protection Act. This external assessment by the Health and Social Care Information Centre consists of a total of 28 requirements covering the following initiatives: Information Governance, Confidentiality and Data Protection, Information Security and Care Records Assurance. The assessment was successfully completed with the Council scoring 100% and a level 3 (the highest score).
- Attendance at Data Protection and Information Management training sessions has resulted in improved staff awareness of information governance requirements and associated organisational processes.

4.2 Leadership and Governance

The SIRO has responsibility for ensuring organisational information risk is properly identified and managed. The SIRO also acts as champion for information risk on the Corporate Management Team and provides an annual SIRO report in regard to information management and risk.

Support for the role is provided by:

- The Chief Privacy Officers (Data Controllers), the Head of Legal and Democratic Services and Head of Customer Services
- The Caldicott Guardians, the Head of Children's Services and the Group Manager for Safeguarding and Community Team

- The Information Asset Owners (Group Managers)
- The Data Governance Advisor

4.3 Training and awareness

The Council has an extensive training programme in Data Protection and Information Governance. In 2014/2015, nineteen training sessions were carried out. These include the Corporate and Induction training sessions and the tailor made sessions after a breach/potential breach.

Additionally, all staff also have to complete the on line e-learning module on Data Protection. Successful completion of this is also a prerequisite for staff receiving their citrix key to enable them to work remotely. 1851 members of staff have completed the mandatory on line 'SPARK' Data Protection e-learning module.

As a part of their Induction session, new Members undertook their Data Protection training on SPARK.

The Data Governance Advisor attended courses in Records Management in November 2013 and Security and Incident Management in June 2014.

One of the Council's Caldicott Guardians achieved her Caldicott Certificate in July 2014.

4.4 Freedom of Information

A total of 1108 requests were received in 2014/2015, compared to 983 in 2013/14. The FOI function sits within the Policy, Engagement and Communication team. The Council replied to 76.26% requests within 20 working days.

4.5 Data Protection

There have been 151 Subject Access Requests (SARs) processed in 2014/2015, compared to 114 processed in 2013/2014. These are requests from customers for copies of their personal data held by the Council. The Council replied to 79.47% of these requests within the 40 day timeline.

A separate log is also maintained of all section 29 requests for third party data from other organisations, including the Police and the DWP. In 2014/2015 there have been 380 requests. These requests were received through Legal and Democratic Services, Revenues and Benefits and the Corporate Policy, Engagement and Communications teams.

The processing of all SARs through the Covalent system commenced in April 2013. This has encouraged consistency in recording; increased efficiency in the monitoring of requests through automatic triggers; enables the maintenance of audit trails and facilitates the production of timely reports.

Increased awareness through the Council's Communications Strategy and extensive training programme continue to improve and highlight the data

protection profile in the Council. This has led to an increase in the reporting of data breaches, which ultimately helps with the continual improvement.

A total of 28 minor incidents were reported for 2014/15. None of them required notification to the ICO. Investigations were undertaken and evaluations with recommendations were made to the SIRO. To mitigate further incidents, follow up work was carried out to ensure recommendations were implemented.

4.6 **Records Management**

All Data Protection training sessions now include aspects of Records Management. This helps to further increase awareness on the secure disposal and archiving of records.

4.7 **Information Security**

There is a comprehensive Information Security Framework to support the current and evolving information security requirements. This ensures that personal data is protected from unauthorised access, loss, damage and destruction. The ICO Audit Action Plan also focussed on a number of security related actions.

The Council continues to have double and, for some applications which are accessed externally, triple password protections.

All Council ICT badged assets are held within the Hornbill system (e.g. asset tag, make and model, number). Any unidentified objects get removed.

In line with Public Service Network compliance, a penetration test was conducted in February 2015 to assess the robustness of the Council's network and this was successfully completed.

Council owned PCs and laptops have Sophos installed to protect against Malware and anti-virus.

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

5.1 The proposed EU Data Protection Regulation has been debated for more than 3 years. The discussion is to continue and the ICO says that the planned timetable will run until December 2015. "If all goes according to that plan, then we'll know pretty much what's going to be in the regulation by the end of this year", the Deputy Information Commissioner wrote in the ICO blog on 26 August 2015. The Data Governance Advisor is to attend a Workshop in October 2015 which will determine the likely changes, what aspects of the Regulation will impact the Council and any possible challenges.

5.2 With on-going Corporate and team restructures and continuing organisational change, 2014/15 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 and meet the requirements of the Local Government Data Handling Guidelines.

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

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