Report to:	Audit and Governance	**Date of Meeting:**	21 September 2016
Subject:	Information Management	**Wards Affected:**	Wards
Report of:	Head of Regulation and Compliance		
Is this a Key Decision?	No	**Is it included in the Forward Plan?**	No
Exempt/Confidential	No		

Purpose/Summary

To update Members on the Council's approach to information management.

Recommendation(s)

1) To note the contents of the report.
2) To request the Head of Regulation and Compliance to submit future reports on an annual basis covering the Council's information management and governance arrangements including details about data breaches within the Council.

How does the decision contribute to the Council's Corporate Objectives?

	Corporate Objective	**Positive Impact**	**Neutral Impact**	**Negative Impact**
1	Creating a Learning Community		x	
2	Jobs and Prosperity		x	
3	Environmental Sustainability		x	
4	Health and Well-Being		x	
5	Children and Young People		x	
6	Creating Safe Communities		x	
7	Creating Inclusive Communities		x	
8	Improving the Quality of Council Services and Strengthening Local Democracy	**x**		

Reasons for the Recommendation:

To inform members of the Council's approach to information governance and management and the consequences of not having appropriate arrangements in place together with details of data breaches in 2015/16.

It is recommended that a similar report is produced on an annual basis.

Alternative Options Considered and Rejected:

None

What will it cost and how will it be financed?

(A) Revenue Costs

N/A

(B) Capital Costs

N/A

Implications:

The following implications of this proposal have been considered and where there are specific implications, these are set out below:

Financial	
Legal Data Protection Act 1998; The EU General Data Protection Regulation	
Human Resources	
Equality	
1. No Equality Implication	x
2. Equality Implications identified and mitigated	
3. Equality Implication identified and risk remains	

Impact of the Proposals on Service Delivery:

Robust information management and governance arrangements will make a positive impact on service delivery throughout the Council.

What consultations have taken place on the proposals and when?

The Head of Corporate Resources (FD 4316/16.....) has been consulted and any comments have been incorporated into the report.

The Head of Regulation and Compliance is the author of the report (LD 3599)

Implementation Date for the Decision

Immediately following the Committee meeting.

Contact Officer: David McCullough
Tel: 934 2008
Email: david.mccullough@sefton.gov.uk

Background Papers:

There are no background papers available for inspection

.

1. Introduction/Background

Sefton recognises information as an important asset in the provision and effective management of services and resources. It is of paramount importance that information is processed within a framework designed to support and enable appropriate information management.

Information Management is a set of multi-disciplinary structures, policies, procedures, processes and controls implemented to manage information at an organisational level, and designed to support regulatory, legal, risk, environmental and operational requirements.

Effective information management should:

- Treat information as a valuable asset;
- Maintain compliance with relevant UK and European Union legislation, for example the Data Protection Act 1998;
- Have in place policies, procedures and guidelines designed to support appropriate information handling and management.
- Demonstrate organisational commitment by setting out roles and responsibilities of staff;
- Have in place appropriately trained Information Governance staff available to provide advice and support to the Council.

2. What Structures Do We have in Place in Sefton

The Corporate Information Management & Governance Executive Group (CIMGEG) is a group of senior Council officers chaired alternatively by the Senior Information Risk Owner (SIRO) and the Head of Commissioning that reports to the Senior Leadership Board (SLB) and the Audit & Governance Committee (A&G). Its role is to oversee the Information Management & Governance framework for the Council.

The following are key membership roles:

- Head of Regulation and Compliance (Joint Chair)
- Head of Commissioning Support and Business Intelligence (Joint Chair)
- Head of Corporate Resources
- Performance and Intelligence Manager
- Data Protection Officer/Caldicott Guardian
- Workforce Learning and Development Manager

The Group has a tactical level group working on their behalf - the Information Management Tactical Group (IMTaG) with representation from the Council's Information Asset Owners (IAOs) and other information specialists.

Other sub groups may be formed as ‘task and finish’ working groups to meet business requirements.

Key roles:

Senior Information Risk Owner (SIRO)

The Council’s SIRO is the Head of Regulation and Compliance and the Deputy SIRO is the Council’s Principal Lawyer. The SIRO is responsible for corporate information risk management and is responsible for leading and fostering a culture that values, protects and uses information in a manner that benefits the Council and its service users.

Information Asset Owners (IAO)

IAO’s are managers who are directly accountable to the SIRO, providing assurance that their information assets are managed effectively in relation to their risks. Specifically duties are:-

- Ensure there is a maintained Info Asset Register for their service area.
- Ensure identification, review and prioritisation of data risks and their mitigation.
- Take instruction from the Council’s SIRO and be actively involved with the Information Management Group.
- Follow the Council’s risk reporting / incident management requirements as published on the intranet.
- Foster an effective Information Governance culture for their staff. This will mean ensuring staff take the Council provided training opportunities and overseeing opportunities for briefing and training within the service area.
- Risk assessment overview. Gain sufficient risk based understanding of their database purposes, what and who enters the data and how it may leave.
- Oversee information risks when a new information asset is being created or imposed.

Information Asset Administrators (IAA)

IAA’s are staff who are familiar with information risks in their area or department. It is not assumed all depts. can afford the resource, or are structured to be able to host this virtual post.

Specifically tasks are:

- Accept delegated tasks from their IAO.
- Act as first port of call for local managers and staff seeking advice on the handling of information.
- Maintenance of Information Asset Registers.

- Ensuring compliance with data sharing agreements, noting day to day issues such as breach near-misses, poor information governance practice.
- Ensuring information handling procedures are fit for purpose and are properly applied especially in relation to personal information.
- Recognise potential or actual security incidents and consult the IAO.
- Under the direction of their IAO, ensure that information is securely destroyed under retention rules.

3. Training

Since July 2014 the Corporate Learning Centre have been providing a half-day briefing session for all council staff entitled 'Information Compliance, Sharing and Guarding'. In that time they have trained 79.8% of all current internal staff which equates to 1875 staff including 128 agency staff and students.

The objectives for the briefing sessions are for staff to:

- Gain a working knowledge of confidentiality and information sharing
- Be aware of relevant legislation and good practice.
- Be aware of security issues for the use and storage of personal information
- Be aware of breaches and the requirement to report breaches immediately

Evaluations from the briefing sessions show that on average 98% of staff rated the session for meeting each objective as excellent or good.

Going forward the plan is to run the briefing sessions every three months for new staff, students and agency staff.

The Corporate Learning Centre are also developing a refresher course as an e-learning package taking approximately 35 to 40 minutes to complete. Following the course is a test of 20 questions with a pass rate of 85%. Staff will be asked to sit this course every two years. Any staff who fail the test will be asked to attend a classroom based briefing session and then re-sit the test.

The E-Learning Refresher course will enable staff to gain a working knowledge of the legislation governing Information Compliance and advice on how to stay within the law when conducting their day-to-day activities including:

- Collecting Information.
- Maintaining Accurate Information.
- Do's & Don'ts when working with information.
- Sharing information.
- Storage & Security of information.
- Information incidents and what to do if it happens to you.

- Rights of Access to Information.
- Direct Marketing and Newsletters.
- Disposal of information

4. Data Breaches

Sefton Council is legally required to take appropriate measures to prevent unauthorised or unlawful processing, accidental loss, and destruction of or damage to personal data.

A data security breach can come in a number of forms such as:

- Loss or theft of data or equipment on which data is stored (laptop, pen drive etc.) whether encrypted or not
- Loss of paper or other hardcopy records, especially where they are lost outside of the office or working environment
- Paper or other hardcopy records are disposed of with inadequate security (placed in with general waste and not sent for shredding)
- Staff member accesses information to which they are not entitled
- Information is obtained by deception
- Information is stolen (emailed or copied without Sefton Council's authorisation)
- Incorrect information is accidentally released (sending sensitive information out to the wrong person or address etc.)

Following guidance from the Information Commissioner's Office (ICO) a serious data breach which has the potential to cause serious detriment / distress to the data subject(s). Loss of sensitive data relating to 10 or more data subjects is deemed serious by the ICO and is classed as a "high risk" factor in the reporting tool we use to report breaches to the Health & Social Care Information Centre (HSCIC).

The Council follows the guidance of the Information Commissioner's Office (ICO) and Health & Social Care Information Centre (HSCIC) guidance on this topic. Specifically the four stages are:

- Containment and Recovery
- Risk Assessment
- Who to notify (data subjects, other agencies, HSCIC, ICO)
- Evaluation, 'Lessons Learned', and Response

A breach or potential breach is not purely an 'internal to the specific department' matter. It is a corporate concern requiring support, to ensure actions or inactions are legal, attend to data subjects' rights, and factor in the Council's reputation and possibility of ICO financial penalties. The ICO currently has the power to impose a civil monetary penalty notice of £ 500,000. However, the new European General Data Protection

Regulation (GDPR) which the UK government may have to adopt in order to demonstrate compliance when trading with the EU, imposes a much higher penalty for serious data breaches. The maximum fine will be up to 10 million Euros or 2 per cent of an organisation's global turnover.

The GDPR also imposes a new duty for all data controllers to report certain types of data breach to the relevant supervisory authority within 72 hours (in the case of the UK this will be the Information Commissioner's Office) and in some cases to the individuals affected. A failure to notify a breach when required to do so may result in a fine.

When a data security incident or breach has occurred, the Data Protection Officer (DPO) should be notified immediately, along with the Information Asset Owner (IAO) of the service involved, relevant senior managers, the Senior Information Risk Owner (SIRO), the Chief Internal Auditor and often a Human Resources representative. The Data Breach Reporting form which is available to all staff on the Intranet must be completed. Data Breach reporting is covered in the Council's mandatory Information Compliance training.

The DPO then convenes a Council Breach Evaluation Group (CBEG) meeting if the breach is deemed serious enough. Otherwise the CBEG is held virtually via e-mail. A minimum of four members of the following are required to make decisions:

- Relevant Department(s) senior manager
- Legal Representative
- Data Protection Officer / Caldicott Guardian
- Where relevant:
    - Human Resources representative; Communications Representative; Specialist Advisors (e.g. IT);
    - Other agencies involved;
    - Chief Internal Auditor (or representative); etc.

The CBEG decide:

- Subsequent containment / recovery actions.
- Whether to disclose the breach to: relevant data subjects; HSCIC / ICO; Other Agency e.g. Police; SIRO or their deputy.
- Internal division of labour, which may include involvement in the investigation or negotiate involvement in any disciplinary investigation.
- Any immediate lessons to be applied in Department or Council.
- Date to meet again regarding meeting all four breach stages (recovery, risk assessment, notification, evaluation).

Example of Enforcement Action Against a Local Authority

In July 2012 a council sold a building which had been previously used as offices for their Children and Adults Services. The property was then vacant but visited by potential buyers for two years until it was sold again in August 14. On 1 September 2014 the company that purchased the property contacted the Council to tell them that they had found 45 bags of confidential documentation in the property. The documentation was found to contain confidential and sensitive personal data relating to over 100 data subjects. The breach was investigated by the Information Commissioners Office who imposed a penalty of £100.000.

Examples of Enforcement Action Against other Public Sector Bodies:

- £180,000 fine for a health trust that twice accidentally disclosed information via email about patients with HIV
- £185,000 fine for a health trust that accidentally published on its internet site personal details of its staff for a period of 11 months.
- £200,000 fine the Crown Prosecution Service after laptops were stolen which contained videos of police interviews.

Sefton position

In 2015/16 the Council experienced 21 Data Breaches and 1"near miss". Of the data breaches 12 were serious enough to warrant reporting to the HSCIC and 1 was classed as a Level 2 breach which was reported and subsequently investigated by the ICO.

SUMMARY OF ALL 22 INCIDENTS

Breach type	**Format**	**Number**
Unauthorised access/disclosure	Digital	5
Unauthorised access/disclosure	Other	1
Disclosed in error	Paper	9
Disclosed in error	Digital	2
Lost or stolen paperwork	Paper	2
Lost or stolen hardware	Digital	2
Near Miss – Disclosed in error	Paper	1
		22

DETAILS OF THE 12 CASES REPORTED TO HSCIC:

Date	Level	Breach type	Format	Comment
01-Apr-15	1	Unauthorised access/disclosure	Digital	Staff member looking at family records
02-July-15	2	Unauthorised access/disclosure	Other	Covert recording of staff member by a service user
03-July-15	1	Disclosed in error	Digital	Court bundle contained information that should not have been disclosed to all parties
01-Oct-15	1	Disclosed in error	Paper	Mis-post of LAC Review notes
06-Oct-15	1	Unauthorised access/disclosure	Digital	Staff member looking at family records
06-Nov-15	1	Disclosed in error	Paper	Paper records contained sensitive information that should not have been disclosed to one of the recipients
18-Nov-15	1	Disclosed in error	Paper	Social care report sent to wrong person
04-Dec-15	1	Disclosed in error	Paper	Misaddressed envelope by Council team containing social care report (children's)
06-Jan-16	1	Disclosed in error	Paper	Child Protection report contained information it should not have
05-Feb-16	1	Lost or stolen hardware	Digital	Laptop stolen from Council office. No encryption due to age of laptop. Minimal information contained on it.
11-Mar-16	1	Unauthorised access/disclosure	Digital	Staff member looking at family records
11-Mar-16	1	Lost or stolen paperwork	Paper	Staff member's address book found outside premises – contained references to service users.

LEVEL 2 BREACH

This breach involved a social worker disclosing confidential and sensitive personal data to a third party who had no legitimate right to have the information. The breach was reported to the ICO who replied as follows:

I write to inform you that I have now completed my investigation into the verbal disclosure of by an individual at Sefton Metropolitan Borough Council ("Sefton MBC"), which was reported on 14 October 2015.

In summary, it is my understanding that this incident concerned a children's social worker who was covertly recorded disclosing confidential and sensitive personal data as defined by the Data Protection Act 1998 (DPA).

Based on the information you have provided, we have decided that regulatory action is not appropriate in this case. The reasons for this are below.

Our consideration of this case.

I have investigated whether Sefton MBC has complied with the requirements of the seventh data protection principle, which states that:

> *"Appropriate technical and organisational measures shall be taken against the unauthorised or unlawful processing or personal data and against accidental loss or destruction of, or damage to, personal data.*

The data in this case is considered to constitute sensitive personal data as defined by the DPA.

Whilst investigating this incident I have considered the seriousness of the breach, aspects of your information governance procedures (such as your policies and training), and the potential detriment to the individuals concerned. It is noted that that our Good Practice team compiled an Audit which was completed in January 2015. Sefton's management accepted the recommendations of the Audit and has confirmed implementation dates for the various recommendations with the ICO.

The follow-up Audit, which was completed in November 2015, identified ongoing concerns regarding training and the monitoring of training within Sefton MBC. The low training completion rate continues to be a cause for concern for the ICO.

However, it is also noted that Sefton MBC has a target of 80% for the uptake in training by April 2016. This commitment has been a factor in the decision not to take regulatory action and we expect Sefton MBC to implement the training as stipulated.

Therefore, after careful consideration and based on the information provided, we have decided not to take any formal enforcement action on this occasion. I would point out that if further information relating to this incident comes to light, or if any further incidents involving Sefton MBC are reported to us, we will revisit this matter, and enforcement action will be considered as a result.

Thank you for your co-operation and assistance during the course of our investigation.

We now consider the matter closed.

Over the past year the number of paper based breaches – particularly in Children's Services - has diminished thanks to better quality control and IT changes. As part of the Council's Data Breach procedures each breach is used to identify possible learning and changes needed. A number of lessons learned have or are being put into practice:

- Core system defaults have been modified to prevent automatic disclosure
- Training provision has been significantly increased
- Provision of specialist bags for conveying paper files
- Potential utilisation of encrypted email (Egress) to ensure secure distribution of sensitive records

The number of breaches caused as a result of human error continues to be a cause for concern. As stated earlier, 79.8% of the current workforce has attended the mandatory Information Compliance training. However, we have recently seen a number of breaches caused by the use of "Auto- Complete" when choosing a recipient's e-mail address in the To, Cc and Bcc fields. In a number of cases, individuals have selected the wrong recipient. The disclosure of personal data to an unauthorised person – that is an individual who has no right to see that information – is a breach of the seventh principle of the Data Protection Act. Data controllers are obliged to take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data against accidental loss or destruction of, or damage to, personal data. The ICO has imposed significant fines on organisations that commit a breach of this nature. Not only due to the failure to take appropriate technical and organisational measures but because the Commissioner considers that the data subjects are highly likely to suffer substantial damage and distress as a result of the unauthorised disclosure. The breach is also highly likely to cause reputational damage to the organisation involved. Monetary penalty notices are published on the ICO's website, are often reported nationally and can result in a loss of public confidence.

The risks associated with not checking the correct e-mail address when working with personal data are highlighted in the Information Compliance training. We are currently looking at technical options as to how to mitigate the risks associated with this type of human error.