Report to:	Audit and Governance Committee	**Date of Meeting:**	6 September 2023
Subject:	Information Governance and Compliance 2022/23		
Report of:	**Executive Director of Corporate Resources and Customer Services**	**Wards Affected:**	(All wards)
Cabinet Portfolio:	Regulatory, Compliance and Corporate Services		
Is this a Key Decision:	No	**Included in Forward Plan:**	No
Exempt / Confidential Report:	No		

Summary:

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

Recommendation(s):

1) To note the contents of the report.

2) To request the Executive Director of Corporate Resources and Customer Services to submit future reports on an annual basis covering the Council's information management and governance arrangements.

Reasons for the Recommendation(s):

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 information compliance in 2022/23.

Alternative Options Considered and Rejected: (including any Risk Implications)

None.

What will it cost and how will it be financed?

(A) Revenue Costs

N/A

(B) Capital Costs

N/A

Implications of the Proposals:

Resource Implications (Financial, IT, Staffing and Assets):

There are no resource implications.

Legal Implications:

- The Freedom of Information Act 2000
- The Environmental Information Regulations 2004
- The UK General Data Protection Regulation
- The Data Protection Act 2018

Equality Implications:
There are no equality implications.

Impact on Children and Young People: No

Climate Emergency Implications:

The recommendations within this report will

Have a positive impact	N
Have a neutral impact	Y
Have a negative impact	N
The Author has undertaken the Climate Emergency training for report authors	Y

Neutral impact. The content of this report is an update to Committee members on information governance and compliance. It does not change the requirement for staff to travel, nor impact upon energy consumption, the amount of water used nor changes green spaces, so has the same impact as we currently do now. It has no impact upon the environment for the communities and stakeholders of Sefton.

Contribution to the Council's Core Purpose:

Protect the most vulnerable: Not applicable
Facilitate confident and resilient communities: Not applicable
Commission, broker and provide core services: To ensure the provision of lawful data processing when providing services
Place – leadership and influencer: Not applicable
Drivers of change and reform: Not applicable
Facilitate sustainable economic prosperity: Not applicable
Greater income for social investment: Not applicable
Cleaner Greener: Not applicable

What consultations have taken place on the proposals and when?

(A) Internal Consultations

The Executive Director of Corporate Resources and Customer Services (FD.7341/23) and the Chief Legal and Democratic Officer (LD.5541/23) have been consulted and any comments have been incorporated into the report.

(B) External Consultations

None.

Contact Officer:	Catherine Larkin
Telephone Number:	0151 934 3286
Email Address:	Catherine.Larkin@sefton.gov.uk

Appendices:

There are no appendices to this report.

Background Papers:

There are no background papers available for inspection.

1. Introduction/Background

Sefton Council 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.

There are a number of pieces of legislation which impose obligations on the Council when managing and handling information, its protection, security, storage, retention and the public's rights with regard to the information the Council holds. The key ones are as follows:

- The Freedom of Information Act 2000
- The Environmental Information Regulations 2004
- The UK General Data Protection Regulation
- The Data Protection Act 2018

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 the UK General Data Protection Regulation and the Data Protection Act 2018;
- 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 and Governance Executive Group (CIMGEG) is a group of senior Council officers chaired by the Senior Information Risk Owner (SIRO) 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:

Senior Manager ICT and Digital (Council's SIRO) (Chair)
Chief Legal and Democratic Officer (Deputy SIRO)
Information Management and Governance Lead (Council's Data Protection Officer)
Workforce Learning and Development Manager
Service Delivery Lead (ICT)

In addition to the Corporate Information Management and Governance Executive group Sefton also has an operational Information Management Group which consists of Information Asset Owners (IAO's) who are managers from across the organisation 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 Information 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.

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

3. Training

The Council first introduced half-day briefing sessions covering information compliance in July 2014 and then moved to a model of online e-Learning in 2016 which all staff must undertake on a refresher basis each year. The module takes approximately 35 to 40 minutes to complete. Following the course is a test of 20 questions with a pass rate of 85%. Staff and Members are required to sit this course every year. Any individual who fails the test will be asked to attend additional information compliance training and then re-sit the test. It is also one of the

mandatory Induction training packages when an employee commences work for the Council.

The eLearning Refresher course enables 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

The course content is reviewed to ensure alignment to best practice and changes in the security risk profile; the next update will include increased information around cyber security, for example. It is anticipated that the new course content will be available later this year in consultation with the IMG Executive.

4. Freedom of Information compliance

The Freedom of Information Act (FOI) provides public access to information held by public authorities. The Act covers any recorded information that is held by a public authority in England, Wales and Northern Ireland, and by UK-wide public authorities based in Scotland. Information held by Scottish public authorities is covered by Scotland's own Freedom of Information (Scotland) Act 2002.

Recorded information includes printed documents, computer files, letters, emails, photographs, and sound or video recordings.

There are 2 separate duties the Council has when responding to requests. These are:

- to tell the person who has made the request (the applicant) whether we hold any information falling within the scope of their request;
- and to provide that information.

A response must be provided within 20 working days unless the Council considers that an exemption applies (for example, the information requested is the personal data of another individual).

Performance analysis (April 2022 – March 2023)

Financial year 2022/23	Numbers
Total Received	1097
Within 20 days response rate	737 (67%)
Outside 20 days response rate	353 (32%)
Requests Withdrawn	7

The number of responses made within the statutory timescale fell in 2022/23 compared to the previous year. However, a proactive improvement plan has been put in place to improve compliance across the Council. The current percentage of responses made within 20 working days is 71%.

In 2022, the Information Commissioner's Office (ICO) set out its commitment to delivering more systemic enforcement action against public authorities that clearly and consistently fail to meet their FOI obligations. Action is regularly taken against public authorities that continue to demonstrate poor FOI performance, including those which demonstrate 'a wilful or negligent attitude to FOI compliance'; those significantly or repeatedly failing to follow the good proactive guidance the ICO publishes; or those that have failed to follow previous advice or comply with lower-level enforcement action. Copies of the Practice recommendations and Enforcement Notices are made available to the public on the ICO's website.

5. Subject access and disclosure requests

Individuals have the right to ask an organisation whether or not they are using or storing their personal information. They can also ask an organisation for copies of their personal information. This is called the right of access and is commonly known as making a subject access request.

The Council received 1,462 subject access requests and disclosures requests in 2022/23. There were 1235 disclosure requests and 227 subject access requests.

The largest number of subject access requests were made to Children's Services, in particular, children's social care (158) followed by Adult Social Care (24). The Council has continued to see a rise in the number of subject access requests received for both departments, for the third consecutive year.

The complexity of such requests differs across the Council, the largest and most complex being those made to Children's Social Care. Individuals have the right to access personal data held about them by an organisation (data controller). In cases where an individual has been in the care of the Local Authority, particularly for the

majority of their childhood, the files can amount to many hundreds of documents, in some cases, thousands. There are currently just 2 employees who handle such 'access to files' requests and disclosures for Adult Social Care (ASC) and Children's Social Care (CSC). In 2022/23, 70% of the subject access requests received by the Council were to Children's Social Care, 11% to Adult Social Care and the remainder were across the rest of the Council.

In 2022/23, the Council saw a total 1,235 requests made outside organisations making requests for disclosure of personal data e.g. the Police, solicitors, NHS, Central Government departments and other Local Authorities.

With regard to disclosure requests, the majority of these requests are received by the Corporate Resource and Customer Services department. In 2022/23 there were 926 requests, which equates to 75% of the total received. For the most part, these are straight forward requests for a limited amount of information, requiring little or no redaction of information prior to disclosure. On the other hand, those made to ASC and CSC by virtue of the nature of the information held within them, are more complex and can require extensive redaction prior to disclosure, for example, removal of third-party information. Requests made to ASC and CSC equated to 24.5% of requests received last year.

6. Data Incidents

Sefton Council is legally obliged 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:

- Information is accidentally released (sending personal data out to the wrong person or address)
- Failing to remove information about an individual before disclosing to another who has no right to see it
- 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)
- Information is stolen (emailed or copied without Sefton Council's authorisation)

The UK GDPR introduced a duty on all organisations to report certain personal data breaches to the Information Commissioner's Office (ICO). Where the incident is considered to be one which must be reported, it must be done within 72 hours of

becoming aware of the breach, where feasible. Guidance from the ICO provides the following by way of a definition:

'*A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data*.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, then those individuals must be informed without undue delay'.

A breach or potential breach is not purely a matter 'internal' to the specific department. 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 enforcement action by the ICO. The Information Commissioner can instruct the Council to take specific steps or actions or stop us from taking certain actions. The ICO also has powers of entry and inspection, can issue warnings, reprimands, enforcement notices and the right to issue civil monetary penalty notices in cases of serious infringements of the legislation. The maximum amount is £ 17,500,000 or 4% of the total annual worldwide turnover of the preceding financial year, whichever is higher.

A failure to notify a breach when required to do so may result in a fine of up to £8.7 million or 2 per cent of an organisation's total worldwide annual turnover (Article 83 of the UK General Data Protection Regulation). The fine can be combined with the Information Commissioner's other corrective powers under Article 58.

Sefton position

Staff have good awareness of information governance as evidenced by the number of reports made to the Council's Data Protection Officer (DPO). In 2022/23, 75 data incidents were reported to the DPO, compared to 54 in 2021/22 and 63 in 2020/21. Of the 75 incidents, 1 was deemed to be an incident which required notification to the ICO. The Council also received 1 complaint from an individual about the handling of their personal data, made via the ICO. No enforcement action resulted from either matter.

The types of incidents experienced by the Council mirrors those of the most commonly occurring breaches across Local Government as reported to the Information Commissioner's Office in 2022/23, which were:

- Data emailed to incorrect recipient
- Data posted or faxed to incorrect recipient
- Failure to redact
- Loss/theft of paperwork or data left in insecure location
- Unauthorised access
- Loss/theft of device containing personal data
- Ransomware
- Verbal disclosure of personal data
- Phishing
- Other

'Non-event' incidents are those reported to the DPO, where, upon further investigation there was no incident, or it was found to be the case that no disclosure of personal data has occurred nor had any been accessed. Such an example would be where an email has been sent to an incorrect recipient, but the email has been retrieved from the unintended recipient prior to opening, or it has been deleted prior to opening. The Council still logs such events to enable lessons to be learned and ensure appropriate recording and training.

Examples of incidents included in the category of 'other' incidents include those where an employee has provided information to an individual but it contains personal data of a third party and the uploading of a case note against the wrong record and loss/theft of an encrypted device.

The vast majority of incidents arise as a result of human error. Any employee who is responsible for a data incident or a 'near miss' must attend additional information compliance training, which is followed up by a one-to-one discussion with a Learning and Development Officer. This covers points of learning and actions the employee will personally take to attempt to prevent a recurrence of the incident for which they were responsible. The Manager of the employee must also investigate the root cause of the incident and confirm the steps they have taken to prevent a recurrence.

The current internal process when a data security incident or breach has occurred, requires the Data Protection Officer (DPO) to be notified immediately, along with the Information Asset Owner (IAO) of the service involved and any relevant senior managers. 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. Various other members of staff may need to be involved, including:

- Relevant Department(s) senior manager
- A Legal Representative
- Human Resources representative
- Specialist Advisors (e.g. IT)
- Communications representative

The CBEG decide:

- Subsequent containment / recovery actions
- Whether to disclose the breach to relevant data subjects, the ICO, other agencies such as the Police
- 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).

7.Data Security and Protection Toolkit (DSPT)

Each year, the Council completes an online self-assessment tool – the Data Security and Protection Toolkit. All organisations that have access to NHS patient data and systems must complete the Toolkit to provide assurance that they are practising good data security and that personal information is handled correctly. The Toolkit forms part of a framework for assuring that organisations are implementing the ten data security standards published by the Department of Health and Social Care, NHS England and NHS Improvement; and that we are meeting our statutory obligations on data protection and data security. Failure to comply with the DSPT requirements could impact on the Council's access to NHS patient data. The Council is currently compliant with the DSPT.

CONCLUSION

In conclusion, over the last 12 months Sefton Council has continued to work hard to meet all of its obligations with information governance and compliance. Clearly, it has been a challenging period which is reflected in the statistics provided in this report. The Council continues to make every effort to improve performance across all areas.