Sefton CVS
Supporting Local Communities

Information Governance Policy, Procedure & Plan

Other relevant CVS policies:
Confidentiality Policy
Network Security Policy

Reviewed:	August 2024
To be Reviewed:	August 2025

CONTENTS

POLICY

PROCEDURE

APPENDICES

<u>POLICY</u>

1. Overview

Sefton CVS considers information to be a vital asset; critical to the efficient management of the organisation, its services and resources. Information plays a key part in supporting governance, service-planning, performance management and compliance. Sefton CVS believes that accurate, timely and relevant information is essential to support high quality service provision and as such, it is the responsibility of all employees (staff, volunteers, associates and contractors) to ensure and promote information quality and to actively use information to improve decision-making wherever relevant.

Sefton CVS recognises the importance of effectively managing individuals' personal information, whether this relates to clients, staff or volunteers, etc. Policies and procedures have been established to ensure that data protection is integral to operational activity; protecting the rights of the individual and discharging the organisation's legal obligations in this regard.

Sefton CVS is committed to maintaining the confidentiality and security of all personal and sensitive data and commercially sensitive information, but acknowledges the need for an appropriate balance between openness and confidentiality in the management and use of information. Sefton CVS recognises that, while every care must be taken to protect the personal information processed, there may also be a need to share client information with partner agencies. This must be done in a controlled manner, consistent with the interests of the client and, in some circumstances, the public interest.

The implementation of an Information Governance framework enables Sefton CVS to review, and improve how it processes (holds, obtains, records, uses, stores and shares) information. This integrates a number of previously separate but inter-related requirements, including:

- Data Protection Act 2018
- General Data Protection Regulation 2016
- The Common Law Duty of Confidentiality
- ISO 27001 Information Security Standard

Information Governance addresses the demands that law, ethics and policy place upon information processing; enabling Sefton CVS to effectively support local communities, by ensuring that information resources are managed, effective and appropriate.

2. Aim

To ensure that information is efficiently managed and that appropriate policies, procedures and management accountability provide a robust governance framework for information management.

3. Scope

This policy covers all information within the organisation; including, but not limited to:

- Client/Service User information
- Personnel information
- Corporate information

All aspects of information handling are covered by this policy, including, but not limited to:

- Structured record systems – paper and electronic
- Transfer of information – e-mail, post, telephone, etc

This policy applies to all information systems purchased, developed and managed by/or on behalf of Sefton CVS and any individual employed, directly or otherwise, by the organisation.

4. Responsibilities

4.1 *Sefton CVS Board*

The Board has ultimate responsibility for the implementation of the provisions of this policy; they are responsible for the management of the organisation and for ensuring that appropriate mechanisms are in place to support service delivery and continuity.

In order to facilitate this, the Board has appointed an Information Governance Champion and an Information Governance Sub-Group has been established *(see Terms of Reference - Appendix 1)*. This sub-group oversees all aspects of Information Governance including the following:

- Data Protection Compliance
- Information Security / Risk Management
- Staff Training
- Business Continuity Planning
- Progress against the NHS IG Toolkit

4.2 *Senior Information Risk Owner (SIRO)*

The SIRO takes overall ownership of the organisations Information Risk Policy; they will champion information risk at Board level and provide advice regarding the effectiveness of information risk management and assurance of the security of information assets.

4.3 *Caldicott Guardian*

The Caldicott Guardian takes the lead on confidentiality issues, ensuring that the organisation satisfies the highest practical standards for handling client identifiable information. They act as the conscience of the organisation, enabling appropriate information sharing and advising on options for lawful and ethical processing of information. They ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff; and oversee all arrangements, protocols and procedures where confidential client information may be shared with external bodies.

4.4 *Information Asset Owners (IAOs)*

Sefton CVS has grouped different categories of information owned by or commissioned by the organisation into 'Information Assets'. An Information Asset Owner has been identified for each information asset; their role is to actively support incident investigations and Information and Confidentiality Audit activity and be responsible for providing assurance to the SIRO on security and risks for their information asset.

4.5 *All Employees*

All employees (staff, volunteers, associates and contractors) are responsible for adhering to Information Governance (IG) policies while carrying out their normal duties and responsibilities. Employees have a duty to familiarise themselves with this policy, abide by its principles, understand and comply with the procedures that support it, report incidents through incident reporting procedures, seek advice and assistance where required and actively participate in mandatory IG training regularly.

5. Commitment & Principles

Ensuring Sefton CVS are equipped to manage Information Governance remains a priority and a suite of distinct policies and procedures have been developed covering all aspects of information handling, including:

- Confidentiality
- Data Management
- Network Security
- Data Incident Reporting
- Data Retention
- Business Continuity

Whilst a key focus is the use of information about clients and the protection of client information; all Information Governance policies apply to information and information processing in its broadest sense and underpin information security and corporate governance.

5.1 Sefton CVS Commitment

- All legislative, contractual, regulatory requirements and national policy will be met
- Appropriate operational procedures exist to support this policy
- Appropriate training will be offered to relevant staff
- The Business Continuity Plan will be maintained and regularly tested

The following factors are critical in order to deliver on these commitments and successfully embed and manage IG across the organisation:

- Commitment from the Board and all staff and volunteers

- Provision of resources and identified support
- Implementation and monitoring of Sefton CVS IG policies
- A commitment to maintain and/or improve Information Governance standards year on year (action plans are derived from the NHS Data Security & Protection Tool Kit).

5.2 IG Principles

Openness

- Non-confidential information on the organisation and its services will be available to the public through a variety of media
- Clients will have ready access to information relating to them in line with their rights
- The organisation will have clear procedures and arrangements for liaison with the press and broadcasting media
- The organisation will have clear procedures and arrangements for handling queries from clients and the public

Legal Compliance *(see Confidentiality Policy/Audit Procedure & Data Management Policy)*

- The organisation regards all identifiable personal information relating to clients and staff as confidential except where national policy on accountability and openness requires otherwise
- The organisation undertakes regular assessments and audits of its compliance with legal requirements relating to Information Governance
- The organisation has established and maintained policies to ensure compliance with the Data Protection Act, the Human Rights Act, the Common Law Duty of Confidentiality and the General Data Protection Regulation.
- The organisation has established and maintained policies for the controlled and appropriate sharing of client information with other agencies, taking account of relevant legislation (e.g. Health & Social Care, Crime & Disorder, Protection of Children, GDPR)

Information Security *(see Network Security, Data Management & Data Incident Policies)*

- The organisation has established and maintained policies and procedures for the effective and secure management of its information assets and resources
- The organisation protects its information assets from all threats, whether internal or external, deliberate or accidental
- The organisation undertakes or commissions annual audits / assessments of its information and IT security arrangements
- The organisation promotes effective confidentiality and security practice to its staff through policies, procedures and training
- The organisation has established and maintained incident reporting procedures and monitors and investigates all reported actual or potential breaches of confidentiality and security

Information Quality Assurance *(see Data Management Policy & Procedure)*

- The organisation has established and maintained policies and procedures for information quality assurance and the effective management of records
- The organisation undertakes or commissions regular assessments and audits of its information quality and records management arrangements
- Information Asset Owners / Managers are expected to take ownership of, and seek to improve, the quality of information they are responsible for
- Wherever possible, information quality should be assured at the point of collection
- The organisation promotes information quality and effective records management

6. Monitoring & Review

This policy will be reviewed on an annual basis or as appropriate and in response to changes to legislation or organisational policies, technologies, increased risks and new vulnerabilities or in response to security incidents.

PROCEDURE

7. Information Security Assurance / Risk Management

Sefton CVS recognises that information security is critical when managing information. In order to ensure that there are adequate controls in place to govern information security particularly in relation to personally identifiable information, Sefton CVS has developed relevant policies and procedures, which are reviewed annually, including:

- Information Governance Policy
- Information Governance Training Strategy
- Data Management Policy & Procedure
  - Master & General Data Retention Policy & Schedule
- Data Incident Reporting Policy
  - Data Incident Reporting Form
- Network Security Policy
  - Access & Authentication Policy
  - Portable / Bring Your Own Device Policy
- Electronic Communication Policy
  - Acceptable Use Policy
  - Social Media Policy

These policies must be followed to minimise the risk of a data and/or network breach. They have been provided to employees and are available on the company website.

A Risk Management Framework is maintained to ensure that any identified risks to information security are monitored and mitigated as far as possible; appropriate penetration testing is carried out on the Sefton CVS network annually.

In order to ensure risk is minimised, data should not be kept for longer than is necessary. All archived data must be appropriately labelled with a destruction date and all data must be disposed of securely. Corporate records are stored and disposed of in accordance with the Master Data Retention Policy & Schedule.

8. Confidentiality & Data Protection Assurance

In order to ensure that Sefton CVS protects confidential information and adheres to relevant legislation (including the Data Protection Act 2018, General Data Protection Regulations 2016, Human Rights Act 1998 and the common law duty of confidentiality), a Confidentiality Policy / Code of Conduct (incorporating the Information & Confidentiality Audit Procedure) has been developed and provided to employees. A copy is also available on the company website.

8.1 Information Audit

All Sefton CVS services / projects have their use of data regularly reviewed as part of an Information Audit; each is assigned to an information asset based on the nature of the data held. Where personally identifiable data is held the legal basis for collection is documented. This is reviewed annually by the Information Asset Owners / IG Lead and monitored by the Information Governance Group.

The information held by Sefton CVS has been split into distinct groupings known as 'Information Assets'. Currently Sefton CVS manages the following information assets:

Information Asset Name	Description of Information Asset
Community Services	Non-health related services delivered / supported by Sefton CVS where data held on the public / non-minority individuals
Equalities Networks	Networks facilitated by Sefton CVS where data held on minority individuals (and also organisations supporting these individuals)
Equalities Services	Services delivered by Sefton CVS where data held on minority individuals / individuals from across the 7 strands of Equality
Health Services	Health related services delivered by Sefton CVS where data held on the public / non-minority individuals
Offender Services	Services delivered for offenders where offender data is held / processed
Organisation Contacts	Services delivered for / to organisations where organisation contact data held
Safeguarding	Safeguarding incident reporting processes (sensitive data held about VCF / SCVS employees / vulnerable adults / children)
Staffing & DBS	General DBS data and Employee / Associate related data including contracts, bank details, staff support and appraisals, PDPs, etc

Training	Training delivery where participant data held
Volunteering	Volunteering services where data held on individuals involved or interested in volunteering
Suppliers	Contractual information relating to third party suppliers where contact / banking details held
IT Systems	Hardware and software installed on the Sefton CVS network – including back-up arrangements

8.2 Information Asset Owners (IAOs)

Each Information Asset has an assigned Information Asset Owner; IAOs receive Enhanced Information Governance training and are generally senior staff members.

IAOs contribute to the Information Asset Register and are responsible for providing assurance to the Senior Information Risk Officer (SIRO) on security and risks for their owned assets. When a data incident or ‘near miss’ occurs the IAO will liaise with the Senior Information Risk Officer to investigate and report on the incident.

8.3 Confidentiality Audit / Compliance Testing

In order to test organisational and individual compliance with the Sefton CVS Confidentiality Policy the coordinates a rolling programme of audit activity as follows:

- SIRO contacts Information Asset Owner/s (IAOs) to discuss audit requirements
- IAOs distribute Staff Compliance Checklists to all employees who have access to their ‘owned’ asset
- IAOs completes relevant documentation and report back to the SIRO on the findings
- SIRO amends Audited Services Improvement Plan as relevant
- SIRO provides access to training where a need is identified

See the Sefton CVS Confidentiality Policy for further details

9. Business Continuity

A Business Continuity Plan (BCP) has been developed; this is reviewed and tested annually to ensure it remains fit for purpose. Testing can involve applying the BCP to an actual incident or scenario-based testing via a table-top exercise.

10. Assessing Performance – NHS IG Toolkit

Adherence to, and assessment against, the online NHS Data Security and Protection Tool Kit ensures that Sefton CVS maintains robust information governance standards and also provides assurance to NHS and other statutory sector commissioners. The Tool Kit is a mandatory self-assessment tool for all NHS contracted services through which organisations demonstrate compliance with NHS Information Governance requirements on an annual basis.

Sefton CVS completes a self-assessment against the defined Toolkit requirements by 31st March annually.

Progress against the Toolkit is monitored in year by the SIRO with regular updates to the Executive Board and the IG Sub-Group. Summary reports and proposed high-level improvement plans are produced annually.

Appendix 1 – Executive Board Information Governance Sub-Group Terms of Reference

Purpose

The purpose of the Information Governance Group is to:

- Ensure compliance with, and oversee implementation of, relevant standards for information governance
- Ensure that Sefton CVS meets the requirements of the NHS Data Security and Protection Tool Kit.

Remit

- To ensure that Sefton CVS has effective policies and management arrangements in place to meet the requirements of:
    - ➢ General Data Protection Regulation 2016
    - ➢ Data Protection Act 2018
    - ➢ Caldicott Principles
    - ➢ Common Law Duty of Confidentiality
    - ➢ Records Management
    - ➢ Information Security
    - ➢ Information Quality
    - ➢ Information Sharing
- To promote the importance of adhering to the law and relevant guidance.
- To establish, implement and monitor an annual information governance work programme as necessary to meet the requirements of the IGT.
- To provide Board assurance through the Information Governance Group that risks associated with Information Governance are being managed and highlight any significant risks and related resource implications.
- To receive and consider reports into breaches of confidentiality and security and other relevant incidents.
- To recommend relevant policies, guidelines and procedures for approval.

Accountability

The primary accountability is to the Sefton CVS Board.

Membership

Board Information Governance Champion
CEO
Deputy Chief Executive / Director of Development
Senior Information Risk Owner / HR & Policy Manager

Caldicott Guardian

Ad hoc membership and attendance from

Responsible Information Asset Owners / Strategic Leads

Quorate

Meetings will be quorate with 50% of members attending.

Deputies

Members of the group will nominate named individuals to deputise in their absence

Frequency of Meetings

Meetings will be held every four months. Other members will be co-opted onto the group for specific input as required.