Policy Name:	SCIL P5 Data Protection & Privacy Policy
Policy Owner:	Risk & Operations Manager
Version Number	v.3.0
Publication Date	19/11/2024
Revision Date	n/a
Approved by:	SCIL Board, 19/11/2024

1. Policy Statement

SCIL is committed to full compliance with the General Data Protection Regulation (GDPR) and the Data Protection Acts 1988-2018 in order to safeguard the rights of our service users and the protection of their data and privacy. SCIL fosters a culture of openness, transparency and accountability in this regard, which is endorsed by the SCIL Board of Charity Trustees.

2. Purpose

This Policy sets out the requirements of SCIL in how we protect our service users' personal data where SCIL acts as a Data Controller and/or Data Processor, and the measures we take to protect the rights of data subjects.

3. Scope

This policy applies to all SCIL employees, work experience visitors, contractors and sub-contractors, third-party suppliers who are authorised to provide services to SCIL, and any other persons or entities when receiving, handling, or processing personal data on behalf of SCIL.

This policy covers all forms of personal data, whether in paper or electronic format, and should be read in conjunction with the SCIL Privacy Notice and SCIL Policy P29 Records Management.

4. Definition

Personal Data means any information relating to an identified or identifiable natural person (the "**data subject**"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or by reference to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

5. Policy

It is the policy of SCIL that all data is processed and controlled in line with the principles of the GDPR and relevant Irish legislation (Data Protection Acts 1988-2018).

5.1 Data Protection Principles

When storing, transmitting, processing or otherwise handling personal data, SCIL commits to ensuring that the data shall be:

- Processed fairly, lawfully and in a transparent manner.
- Obtained and processed only for specified, explicit, lawful, and legitimate purposes.
- Limited to what is necessary in relation to the purposes for which it is processed.
- Accurate and kept up to date where necessary.

- Retained only for as long as is necessary for the purposes for which it is processed.
- Processed in a secure manner, which includes having appropriate technical and organisational measures in place to prevent and/or identify unauthorised or unlawful access to, or processing of, personal data, and to prevent accidental loss or destruction of, or damage to, personal data.

Data subjects under GDP have the right to:

- Request access to their data through a Subject Access Request (SAR).
- Request the correction of any inaccurate data.
- Object to having their data processed.
- Request the deletion of their data.
- Request to have their data moved if it is in electronic format.

SCIL does not employ any automated processing of personal data and will only transfer personal data to third parties within Ireland in accordance with this policy. It does not transfer data outside of the European Economic Area (EEA).

SCIL will communicate with data subjects in a concise, transparent, intelligible and easily accessible form, using clear language.

5.2 Legal Basis for Processing Personal Data

SCIL has a lawful basis for processing the above information as follows:

- The processing of the data is necessary to protect service users' vital interests (the "data subject") as per Article 6(1)(d) of the GDPR. This is to ensure that we have full regard to any information that is relevant and/or necessary for us to safely provide our services.
- The processing of the data is required as part of our provision of services to the HSE, Túsla or other healthcare or disability service, the "data controller". This is in scenarios where SCIL has been commissioned to provide services by such an agency, and the data we process is relevant and necessary for the provision of those services.

We will only process special categories of personal data where it is necessary for the provision of healthcare, disability services or social care or where it is required under contract with a healthcare or disability service such as the HSE, Túsla, or another third-party agency.

Processing is lawful where it is undertaken by or under the responsibility of a person who in the circumstances owes a duty of confidentiality to the data subject.

Special categories of data are defined by the GDPR and include data such as racial or ethnic origin, religious or philosophical beliefs, health data, sex life details and sexual orientation. The processing by SCIL of special categories of personal data shall be lawful where it is necessary:

- for the assessment of the working capacity of an employee,
- for the provision of health and social care,
- for the management of health or social care systems and services, or
- pursuant to a contract with a health professional.

5.3 Data Storage Limitation Policy

SCIL will erase any personal data that violates Data Protection Law/Regulations or contractual obligations, or where SCIL no longer requires the data.

5.4 Data Anonymisation and Pseudonymisation

SCIL will anonymise or pseudonymise personal data when it is being used for purposes other than the direct provision of its healthcare and disability services.

5.5 Unauthorised Disclosure / Loss / Alteration of personal data

All persons covered under this policy are prohibited from disclosing a data subject's confidential information (including personal data or special categories of personal data), unless this policy or a legal basis allows for such disclosures. All persons covered under this policy must report to the Data Protection Officer all suspected incidents of unauthorised disclosure, loss, destruction or alteration of service users' personal information. Incidents should be reported as soon as possible after discovery to allow for investigation and corrective action where necessary to minimise any impact to the data subject(s) or risk to others.

5.6 Data Protection by Design

SCIL aims to apply the principles of Data Protection by Design throughout its systems and processes to ensure that data protection requirements are built in from the outset and are kept up to date throughout the lifecycle of our services. A Data Protection Impact Assessment is carried out by the Data Protection Officer when the introduction of or amendment to a service or process "is likely to result in a high risk to the rights and freedoms of natural persons" (per GDPR).

5.7 Third Parties Relationships Policy

SCIL may engage third party data processors for the provision of a healthcare management system and other ancillary support services. We ensure these parties protect personal data through sufficient technical and organisational security measures and take all reasonable steps to ensure GDPR compliance.

5.8 Education and Awareness

SCIL provides data protection training and induction to all employees on joining the organisation.

6. Roles and Responsibilities

6.1 SCIL Board of Directors

The SCIL Board of Directors is the formal sponsor of this policy, reflecting the importance of GDPR compliance in the organisation and the priority afforded to protecting personal data. The Board delegates the day-to-day oversight and implementation of this policy to the Data Protection Officer who provides regular reporting to the Board via the SCIL Risk Committee.

6.2 The Data Protection Officer

The data protection officer (DPO) is responsible for overseeing this policy and the protection of personal data in SCIL, and for monitoring GDPR compliance in the organisation. This will include reviewing processing activities, carrying out Data Protection Impact Analysis work where required, and providing formal reporting to the Board of Directors on any data protection issues or incidents requiring escalation.

7. Enforcement

SCIL staff who breach this policy may be subject to disciplinary action as provided for in the SCIL disciplinary procedure. If a breach occurs due to reckless behaviour and is knowingly not reported, the person responsible may be held accountable. SCIL reserves the right to take such action as it deems appropriate against individuals who breach the conditions of this policy.

Where a breach of this policy is committed by contractors, sub-contractors, agency staff or third-party service providers, SCIL reserves the right to take remedial actions via the contracts in existence.

8. Policy Governance

This policy will be reviewed and updated every 3 years or more frequently if necessary to ensure it is kept up to date and relevant to SCIL's organisation structure and business practices at the time.

9. Version History

	Date	Details of Changes	Approval
v2	n/a	Policy drafted by SON consultancy in preparation for HIQA readiness.	n/a
v3	19/11/2024	Redrafted to merge GDPR/Data Protection/Confidentiality.	SCIL Board 19/11/2024

10. Appendix I – Glossary of Terms

Term	Definition
Anonymised	The process of making personal data anonymous data.
Anonymous Data	Any information relating to a natural person where the person cannot be identified whether by the Data Controller or by any other person, taking account of all the means reasonably likely to be used either by the Data Controller or by any other person to identify that individual.
Consent	Any freely given indication of a data subject's agreement to the processing of personal data relating to them. Consent is typically a specific, informed and unambiguous written statement or a clear affirmative action.
Data	Information which is recorded either digitally or I manual (paper) format as part of a relevant filing system.
Data Controller	A person or organisation who (alone or with others) determines the purposes for which and the manner in which any personal data are, or are to be, processed. A Data Controller can be the sole Data Controller or a joint Data Controller with another person or organisation.
Data Processor	A person or organisation that holds or processes personal data on the instructions of the Data Controller, but does not exercise responsibility for, or control over the personal data.
Data Protection	The protection of personal data
Data Protection Commission	The office of the Data Protection Commission in Ireland.
Data subject	The individual to whom personal data held relates, including employees, customers, and suppliers.
DPO	Data Protection Officer
EEA	European Economic Area Means the area in which the Agreement on the EEA provides for the free movement of persons, goods, services and capital within the European Single Market, as well as the freedom to choose residence in any country within this area.
Encryption	The process of encoding information stored on a device and can add a further useful layer of security. It is considered an essential security measure where personal data is stored on a portable device or transmitted over a public network.
EU Directive	Means the EU Data Protection Directive 95/46/EC.
Personal Data	Any information relating to an identified or identifiable natural person (Data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or by reference to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Processing	Any operation performed on personal data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. This includes manual and automated operations.
Pseudonymisation	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to

	ensure that the personal data are not attributed to an identified or identifiable natural person.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
Restriction of Processing	The marking of stored personal data with the aim of limiting their processing in the future.
Subject Access Request	A written request made by any individual about whom SCIL keeps personal data on computer or in a relevant filing system. Response must be provided to the data subject under the terms outlined by GDPR.
Third Party	An entity that is in a contractual arrangement with SCIL to provide products and services. Third Party relationships, for the purposes of this policy, generally do not include customer relationships. Under GDPR a 'Third Party' means a natural or legal person, public authority, agency or body, other than the data subject, controller, processor and persons who, under the direct authority of the Data Controller or Data Processor, are authorised to process personal data.