GDPR and Retention Policy

1 Introduction

At Step Into Learning (SIL), we prioritise the responsible handling of personal information throughout our operations. Whether concerning our employees, students, or external parties such as customers, contractors, and suppliers, safeguarding this data is integral to our commitment to integrity and compliance.

This policy delineates our approach to acquiring, managing, and utilising personal data, whether in physical or electronic formats. We are dedicated to ensuring that all data under our purview is treated with the utmost care and in accordance with applicable laws and regulations, particularly the General Data Protection Regulation (GDPR).

2 Scope

This policy applies to all aspects of SIL's operations where personal data is involved. This encompasses the acquisition, storage, usage, and disposal of such data, regardless of the medium it is stored in. Whether it pertains to internal processes, interactions with stakeholders, or provision of goods and services, adherence to this policy is mandatory.

Furthermore, this policy extends to all individuals within SIL who may come into contact with personal data in the course of their duties, including employees at all levels, contractors, and third-party service providers.

By outlining clear guidelines and procedures, this policy ensures that personal data is handled securely, and that its retention is limited to what is necessary for the fulfilment of our obligations and objectives.

Decisions regarding the retention and disposal of documents containing personal data must align with the principles outlined in this policy.

Upon the expiration of a document's retention period, a review must precede its disposal. This review need not be overly time-consuming or complex. Should a decision be made to dispose of a document, careful consideration must be given to the method of disposal.

This policy applies universally to all personal information processed by SIL, irrespective of storage methods or the individuals to whom the data pertains. This includes past and present employees, job applicants, contractors, clients, and supplier contacts.

3 Definitions

Criminal records information encompasses personal data concerning criminal convictions, offences, allegations, legal proceedings, and associated security measures.

Legitimate Interests Assessment (LIA) refers to an evaluation of SIL's legitimate interests, the necessity of processing to achieve those interests, and the balance with the rights, freedoms, and interests of individuals.

Personal information, also referred to as personal data, pertains to information concerning an identifiable individual, whether directly or indirectly.

Processing entails any action involving personal information, including obtaining, recording, organising, storing, modifying, retrieving, disclosing, or destroying it.

Pseudonymised denotes the process of processing personal information in a manner that prevents direct identification of individuals without supplementary information, which is securely maintained separately and subject to technical and organisational safeguards to ensure the continued anonymity of the data.

4 Policy Statement

Step Into Learning (SIL) is committed to adhering strictly to lawful grounds for the retention and processing of personal information. Before commencing any processing activity and periodically thereafter, the following steps will be taken:

Assessment of Lawful Reasons:

We will review the purposes of the processing activity and select the most suitable lawful reason(s) for the processing, which may include:

- Consent from the data subject (only applicable in specific circumstances).
- Necessity for the performance of a contract with the data subject or for pre-contractual measures.
- Compliance with legal obligations binding on SIL.
- Necessity for the legitimate interests pursued by SIL or a third party, ensuring that these interests do not override the rights and freedoms of the data subject.
- For processing of criminal records information, a lawful condition for processing will be identified and documented.

Assessment of SIL's Legitimate Interests:

When considering SIL's legitimate interests as the grounds for lawful processing, a Legitimate Interests Assessment (LIA) will be conducted and documented to substantiate our decision.

If the LIA reveals a significant privacy impact, the necessity of conducting a Data Protection Impact Assessment (DPIA) will be evaluated.

The LIA will be periodically reviewed and repeated as needed in response to changing circumstances.

5 Accountability

Step Into Learning (SIL) ensures adherence to data protection principles through the implementation of policies, codes of conduct, and relevant procedures.

Data Subjects' Rights:

SIL facilitates data subjects in exercising their rights under the UK GDPR, including:

- Access to personal data and information regarding processing.
- Data portability.
- Rectification.
- Erasure ('right to be forgotten').
- Restriction.
- Objection.
- Prevention of automated decision-making.
- Compensation.
- Complaints to the Commissioner.

Data subjects have the right to lodge complaints regarding the processing of their personal data with SIL, subject to the terms of SIL's Complaints Procedure.

Consent:

Consent must be explicitly given, informed, and unambiguous.

Withdrawal of consent is permitted at any time.

In cases where the data subject lacks competence to provide consent, processing requires authorisation from the individual's next of kin as recorded on the SIL MIS system.

Approved consent forms must be used for obtaining consent to process personal and special category data.

Data Security:

All employees are responsible for safeguarding data access and must adhere to protocols preventing inappropriate sharing of personal data.

Access to SIL information systems or records is permitted solely for fulfilling contractual duties.

Personal data must be securely managed, with manual records subject to specific guidelines for storage, access, and disposal.

Data retention and disposal must adhere to the Data Retention Schedule.

Disclosure of Personal Data:

Personal data shall not be disclosed to third parties without appropriate authorisation.

SIL shares personal data with government and other agencies only where necessary and as outlined in privacy statements or notices.

Data shared with recipients must be accurate and complete, and recipients must handle the data in accordance with their privacy policies.

Data Transfers:

Personal data transfers outside the UK require safeguards such as adequacy decisions, Standard Contractual Clauses (SCCs), or Binding Corporate Rules.

Exceptions to safeguards necessitate explicit consent or other lawful bases for transfer.

Risk and Impact Assessments:

SIL conducts assessments to evaluate risks to data subjects' rights and freedoms.

External Data Processors and Cloud Computing:

IT and DPO authorisation are required for external data processing.

Data Sharing Agreements must be established prior to processing.

External processing is subject to oversight by designated SIL managers and internal auditors.

Partnership Working:

Written data sharing agreements are required for partnership activities involving personal data.

Designations as Data Controller, Joint Data Controller, or Data Processor must be clearly defined.

Customer Service:

Data protection regulations should not hinder excellent customer service.

Correct, compliant approaches will be pursued in assisting individuals while ensuring information security.

Retention:

SIL adheres to its Retention and Disposition Policy and Data Retention Schedule.

Personal data is retained for necessary periods and securely disposed of when no longer required.

Data Protection Impact Assessment (DPIA):

DPIAs are conducted for projects or processes posing risks to personal data.

SIL evaluates DPIA necessity based on specified criteria outlined by the ICO and the UK GDPR.

Regular review of DPIAs is conducted post-approval and implementation.

Data Subject Access Requests (DSAR):

Data subjects have the right to access their personal data held by SIL.

SIL verifies the identity of data subjects making access requests.

Personal data is retained in compliance with the UK GDPR, and DSARs are handled according to SIL's Data Subject Access Procedure.

6 Storage and Retention

Step Into Learning (SIL) ensures the secure storage and retention of personal information, including sensitive personal information, in accordance with GDPR regulations.

The duration for which data is retained will vary based on circumstances, including the purposes for which the personal information was acquired and relevant legal, regulatory, or business considerations (refer to Appendix 1).

Personal information, including sensitive personal information, no longer necessary will be permanently deleted from our information systems, and any hard copies will be securely destroyed.

To uphold SIL's obligations concerning the storage and retention of personal data, it is imperative not to maintain personal information in a form that enables the identification of individuals beyond the legitimate business purposes for which it was collected.

7 Responsibility

The Data Protection Officer (DPO) is tasked with maintaining the retention schedule, ensuring its alignment with evolving business requirements, updated legislation, evolving risk management perspectives, and shifting business priorities.

In accordance with this policy, the DPO is responsible for assessing whether to retain or dispose of specific documents.

The operational aspects of this function may be delegated by the DPO to any trusted member of SIL.

8 Organisations with which Personal Data may be shared

Protecting your personal data is vitally important to us and we share your information only when necessary and where there is a lawful basis to do so according to Article 6 of the UK GDPR. SIL may share data and information with:

Organisation Name	Organisation Role	Function
TERMS	Software supplier	Processor

SAGE	Software Supplier	Processor
ITP Systems	Analytics Software supplier	Processor
Careers Southwest	Careers Service	Processor
Cornwall County Council	Service provider (Element 3)	Controller
Plymouth County Council	Service provider (Element 3)	Controller
Devon County Council	Service provider (Element 3)	Controller
CPOMS	Software provider (safeguarding)	Processor
Disclosure and Barring service	DBS check provider	Processor
Egress	Software supplier	Processor
Education Skills Funding Agency	Government department	Controller
Department for Education	Government department	Controller
Department of work and Pension	Government department	Controller
Cornwall Learning Partnership	Service Provider	Controller
Transferable Skills Training	Training Provider	Processor
Cornwall Neighbourhood For Change	Training Provider	Processor
The Outdoor Place	Training Provider	Processor
AIM	Service Provider	Processor
OCNL	Service Provider	Processor
NCFE	Service Provider	Processor
HMRC	Government department (payroll)	Controller

9 Disposal

Step Into Learning (SIL) is committed to securely disposing of personal data when it is no longer required to mitigate the risk of inaccuracies, outdated information, or irrelevance.

The method of disposal will be selected based on the nature and sensitivity of the documents and includes:

- Confidential paper waste is collected and disposed of by Lyreco or trusted online storage providers.

- SIL will retain certain forms of information for varying durations. Information about learners will be kept for 10 years after they leave the course, extended to 31/12/2030 for ESF 2014-2020 match funding, including all ILR documentation.
- General staff information will be retained for 5 years after they leave, with specific information such as pensions, taxation, and reference-related data kept for longer periods.
- Non-confidential records may be placed in wastepaper bins for disposal.
- Deletion of computer records will be conducted securely.
- Transmission of records to external bodies will be managed securely.
- Cloud storage will be utilised for secure storage and transmission of records.

10 Document Control

We are ISO 9001 Quality Management and ISO 14001 Environmental Management standards compliant. We review all documents annually (or at set intervals like monthly/quarterly as appropriate to the document) and make decisions based on the review. Previous versions or defunct documents are moved to an Archive folder where they are retained for 7 years.

11 Appendix 1

Commercial contracts:

Type of record	Retention period	Where is it stored?	Reason	Method of Deletion
Contracts with Funding Bodies	7 years after last action	Digitally Hard Copy	Contractual	Deletion Confidential waste
Contracts with Partners	7 years after last action	Digitally	Legal	Deletion
Purchase orders and invoices	7 years after last action	Digitally Hard Copy	Legal	Deletion Confidential waste
Accounting & financial management information	6 years from end of fiscal year	Digitally	Legal	Deletion

Email records:

Type of record	Retention period	Stored	Reason	Method of Deletion
Email correspondence	Archive emails after 6 months	Digitally	Legal	Archive on the computer

Employment records: please see Recruitment retention.

Type of record	Retention Period	Stored	Reason	Method of Deletion
PAYE records	3 years from end of fiscal year	Digitally	Legal	Deletion
Medical and health records	3 years after employment ceases	Digitally	Legal	Deletion
Unsuccessful candidates	6 months after last action	Digitally	Legal	Deletion
Accident report forms	3 years after last action	Digitally	Legal	Deletion
Employment records: redundancy, equal opportunities; health & welfare records	6 years after last action	Digitally	Legal	Deletion
Pay & tax: pay deductions, tax forms, payroll, loans	6 years after last action	Digitally	Legal	Deletion
Records of formal disciplinary actions in employee file	6 years after last action	Digitally	Legal	Deletion
Records of formal grievances in employee file	6 years after last action	Digitally	Legal	Deletion

Operational records:

Type of Record	Retention Period	Stored	Reason	Method of Deletion
Fire Risk Assessments	Retain until superseded	Digitally	Legal	Deletion on computer
Policies/Procedures	7 years	Digitally	Legal	Deletion on computer
Complaints	6 years from end of fiscal year	Digitally	Legal	Deletion on computer
Building (i.e. lease/deeds)	Destroy 6 years after property is no longer occupied]	Digitally	Legal	Deletion on computer
Maintenance contracts	15 years from last action	Digitally	Legal	Deletion on computer
Insurance schedules	10 years after last action	Digitally	Legal	Deletion on computer
Register of Trustees	Life of company	Digitally	Legal	Deletion on computer
Employer's liability insurance certificates	Life of company	Digitally Hard Copy	Legal	Deletion Confidential Shredding

Learner Records

in accordance with the ESF 2014-2020 match funding rules some of the document below need to be kept until 2034

Type of record	Retention period	Stored	Reason	Method of Deletion
Applications	2 years	Digitally Hard Copy	Legal	Deletion on computer Confidential Shredding

Certificates	31/12/2034 or 7 years for ILP after academic year 2020	Digitally Hard Copy	Legal	Deletion on computer Confidential Shredding
ILR	31/12/2034 or 7 years for ILP after academic year 2020	Digitally Hard Copy	Legal	Deletion on computer Confidential Shredding
ILP	31/12/2034 or 7 years for ILP after academic year 2020	Digitally Hard Copy	Legal	Deletion on computer Confidential Shredding
Programme Work	7 years	Digitally Hard Copy	Legal	Deletion on computer Confidential Shredding
Personal Files	7 years	Digitally Hard Copy	Legal	Deletion on computer Confidential Shredding

Field	Description
Document title	GDPR and Retention Policy
Version	V9.0
Author	Business Support
Date issued	09/05/2025
Status	Approved
Approved by	Trustees
Review date	09/05/2026
Document location	Document Control SharePoint - Data