South West Learning – Data Protection and GDPR Policy

Introduction and Purpose

South West Learning (SWL) recognises its legal and ethical responsibilities under the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR) (together referred to as the *Data Protection Laws*).

As an organisation providing educational and tutoring services to children and young people aged 11–16, SWL collects and processes personal data relating to students, parents, staff, contractors, and partner schools. We are committed to ensuring that all personal data is handled lawfully, fairly, transparently, and securely.

This policy outlines how SWL complies with the Data Protection Laws and should be read alongside the SWL Data Protection Procedures, Safeguarding and Child Protection Policy, and Confidentiality Statement.

This policy applies to all SWL employees, tutors, contractors, volunteers, and Directors who process or have access to personal data on behalf of South West Learning.

It covers all personal data held by SWL in both digital and paper formats, including but not limited to:

- Student and parent information
- Employee and tutor records
- Client and partner school details
- Financial and administrative information

Definitions

The following definitions apply within this policy:

- Personal Data: Any information relating to an identifiable individual (e.g. name, contact details, identification number, or other factors specific to their identity).
- Special Category Data: Sensitive personal data such as racial or ethnic origin, religious beliefs, health information, or sexual orientation.
- Processing: Any operation performed on personal data, such as collection, storage, use, disclosure, or deletion.
- Data Controller: The organisation that determines the purposes and means of processing personal data (SWL).
- Data Processor: A third party that processes data on behalf of SWL.
- Data Subject: The individual to whom the personal data relates (e.g. student, parent, staff member).
- Personal Data Breach: A security incident leading to loss, unauthorised disclosure, or misuse of personal data.
- Consent: A freely given, specific, informed, and unambiguous agreement to the processing of personal data.

Data Protection Principles

Under the Data Protection Laws, SWL must process personal data in accordance with the following principles. Personal data must be:

- Processed lawfully, fairly, and transparently
    - Data subjects are informed about how their data will be used.
- Collected for specified, explicit, and legitimate purposes
    - Data will not be used for reasons incompatible with the purpose for which it was collected.
- Adequate, relevant, and limited to what is necessary
    - Only the data required for operational or legal purposes will be collected.
- Accurate and kept up to date
    - Inaccurate data will be corrected or deleted without delay.
- Kept for no longer than necessary
    - Data will be retained in line with SWL's retention schedule and deleted securely when no longer required.
- Processed securely
    - Data will be stored and handled using appropriate technical and organisational measures to prevent loss, unauthorised access, or damage.
- Accountability
    - SWL is responsible for and must be able to demonstrate compliance with all principles.'

Lawful Bases for Processing

SWL will only process personal data when a lawful basis applies, including:

- Consent: The individual has given clear consent for a specific purpose.
- Contract: The processing is necessary for the performance of a contract (e.g. tutoring agreement).
- Legal Obligation: To comply with legal requirements (e.g. safeguarding or tax legislation).
- Vital Interests: To protect someone's life or safety.
- Public Task: For duties carried out in the public interest (e.g. education provision).
- Legitimate Interests: Where processing is necessary for SWL's legitimate activities and does not override the rights of individuals.

Special category data (such as medical or safeguarding information) will only be processed where additional conditions under UK GDPR Article 9 are met (e.g. explicit consent or safeguarding necessity).

Data Subject Rights

Individuals have the following rights under the Data Protection Laws:

- Right to be informed – to receive clear information on how their data is collected and used.
- Right of access – to request a copy of the personal data held about them.
- Right to rectification – to request correction of inaccurate or incomplete data.

- Right to erasure ('right to be forgotten') – to request deletion of personal data where lawful grounds allow.
- Right to restrict processing – to request limitation of data use.
- Right to data portability – to receive their data in a structured, machine-readable format.
- Right to object – to object to processing based on legitimate interests or direct marketing.
- Rights in relation to automated decision-making and profiling – SWL does not use automated decision-making systems.

Requests relating to these rights must be submitted in writing to the Data Protection Lead (see contact details below). SWL will respond within one month of receipt unless an extension is necessary due to complexity.

Privacy Notices

SWL provides clear and accessible Privacy Notices whenever personal data is collected — whether directly from the individual or indirectly via a partner organisation (e.g. school or local authority).

Privacy Notices outline:

- What information is collected
- The purpose of processing
- The lawful basis
- Data retention periods
- Data sharing arrangements
- Contact details for queries or complaints

Data Security and Confidentiality

SWL will take appropriate technical and organisational measures to ensure the security of all personal data. These include:

- Password protection and multi-factor authentication for electronic records.
- Secure, encrypted storage for all personal and safeguarding data.
- Restricted access to authorised personnel only.
- Regular data backups and secure disposal of obsolete files.
- Confidentiality agreements for all staff and contractors.

All staff are required to complete annual Data Protection and Cyber Security Training and to report suspected breaches immediately.

Data Breaches

A personal data breach is any incident that results in unauthorised access, loss, alteration, or disclosure of personal data.

In the event of a breach:

- The Data Protection Lead must be informed immediately.
- SWL will investigate, take steps to contain and mitigate the breach, and assess the level of risk.
- Where the breach is likely to result in risk to individuals' rights and freedoms, the Information Commissioner's Office (ICO) will be notified within 72 hours.
- Affected individuals will also be informed where there is a high risk of harm.

All breaches and near misses will be recorded in the Data Breach Register and reviewed to prevent recurrence.

Data Retention and Disposal

Personal data will only be retained for as long as necessary for legal, safeguarding, or operational reasons. Retention periods include:

- Student and tutoring records: 7 years after service completion
- Safeguarding records: Retained in line with statutory guidance
- Employee and contractor records: 6 years after employment ends
- Financial data: 7 years for tax and audit purposes

Data no longer required will be securely deleted, shredded, or anonymised.

Third-Party Processing

SWL may share personal data with third parties where necessary for service delivery or legal compliance (e.g. local authorities, schools, DBS, accountants, or IT providers).

Before sharing, SWL ensures:

- The third party has a lawful reason and appropriate safeguards.
- A Data Processing Agreement is in place.
- Data is shared on a "need to know" basis only.

SWL does not sell or transfer personal data to third parties for marketing purposes.

Data Protection by Design and Default

SWL integrates data protection into all new systems, procedures, and projects. This includes:

- Conducting Data Protection Impact Assessments (DPIAs) where required.
- Applying data minimisation principles.
- Using pseudonymisation and encryption where possible.
- Reviewing data-handling systems for security and compliance.

Training and Awareness

All staff, tutors, and contractors receive induction and refresher training on:

- Data protection principles
- Confidentiality and record keeping
- Secure information handling
- Reporting data breaches

Training records are maintained and monitored by the Data Protection Lead.

Complaints and Concerns

Individuals who have concerns about how their personal data is handled should contact the Data Protection Lead in the first instance.

If unresolved, complaints may be escalated to the Information Commissioner's Office (ICO):
ICO Helpline: 0303 123 1113 Website: www.ico.org.uk

Communicating this Policy

This policy will be:

- Shared with all staff, tutors, and contractors during induction.
- Available on request to clients, schools, and parents.
- Reviewed annually and updated where legislation or guidance changes.

Contact Details:

- South West Learning
- Email: info@southwestlearning.co.uk
- Designated Safeguarding Lead: Emma Radford
- Deputy DSL: Eleanor Hoggett

Policy Review

This policy will be reviewed annually, or sooner if statutory updates require, by the Directors and DSL.

Date Approved: September 2025

Date for Review: September 2026