Data Protection Policy

Green-State Innovation and Training Ltd (G-SIT Ltd)

Document Control

Reviewed: 29 September 2025

Next review due: 29 September 2026

Review frequency: Annually

1. Purpose and Scope

This policy sets out how Green-State Innovation and Training Ltd (G-SIT Ltd) protects personal data. It applies to all staff, contractors, and partners who process personal data on our behalf, across all activities and systems.

2. Legal Framework

We comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

The Data (Use and Access) Act 2025 (DUAA) introduces targeted amendments to UK GDPR, DPA 2018 and PECR. Changes are phasing in between June 2025 and June 2026.

We also follow the Privacy and Electronic Communications Regulations (PECR) for electronic marketing and cookies.

3. Key Definitions

Personal data: Information relating to an identified or identifiable person.

Special category data: Personal data revealing e.g. health, ethnicity, beliefs, etc.

Controller / Processor: We act as controller for our own activities; third parties may act as processors under our instructions.

4. Data Protection Principles (Article 5 UK GDPR)

Lawfulness, fairness and transparency

Purpose limitation

Data minimisation

Accuracy

Storage limitation

Integrity and confidentiality (security)

Accountability – we are responsible for and can demonstrate compliance with all principles.

5. Lawful Bases for Processing

We will establish and record at least one lawful basis before processing personal data:

Consent

Contract

Legal obligation

Legitimate interests (with balancing test)

Vital interests (rare)

Public task (where applicable)

6. Roles, Responsibilities and Governance

The Board and senior management oversee compliance. Managers must ensure their teams follow this policy.

Where we are not legally required to appoint a Data Protection Officer (DPO), we designate a Data Protection Lead as the main contact for data protection matters.

Data Protection Lead: [insert name/email/phone]

Information governance: training for all staff on induction and at least annually

Records of Processing Activities (RoPA) maintained and reviewed

Data Protection Impact Assessments (DPIAs) for high-risk processing

7. Individuals' Rights

We enable the following rights, subject to legal exemptions:

To be informed (privacy notices)

Access (Subject Access Requests) – normally within one month; we may 'stop-the-clock' while awaiting clarification or ID

Rectification

Erasure (where applicable)

Restriction

Data portability (where applicable)

Object (including to direct marketing)

Withdraw consent at any time (where processing is based on consent)

Complain to the Information Commissioner's Office (ICO)

8. Minimisation, Accuracy and Retention

Collect only what is necessary for specified purposes

Keep data accurate and up to date; correct or delete inaccuracies promptly

Retain data only as long as necessary in line with our retention schedule; securely dispose of data when no longer needed

9. Security and Confidentiality

Access controls and role-based permissions

Encryption in transit and at rest where appropriate

Pseudonymisation/anonymisation where feasible

Secure configuration, patching and malware protection

Physical security for premises and records

Supplier due diligence and contractual controls

Staff training and acceptable-use rules

10. Processors and Data Sharing

We appoint processors only with appropriate due diligence

We put in place Article 28-compliant contracts with processors (including confidentiality, security, sub-processor approvals, assistance with rights and breaches)

We document data sharing with other controllers and use appropriate agreements

11. International Transfers

We make restricted transfers outside the UK only with appropriate safeguards, typically the UK International Data Transfer Agreement (IDTA) or the UK Addendum to the EU Standard Contractual Clauses, supported by transfer risk assessments (TRAs).

12. Direct Marketing and Cookies (PECR)

Electronic marketing (email/SMS) only with the appropriate lawful basis and consent where required; always provide an opt-out

Maintain suppression lists and honour opt-outs promptly

Provide clear and accessible cookie information and controls on our websites/apps; respect user choices

13. Children and Vulnerable Individuals

Use age-appropriate notices and obtain parental consent where required

Apply enhanced safeguards for vulnerable learners and safeguarding records

14. Personal Data Breaches

Report suspected breaches immediately to the Data Protection Lead

Log, investigate and assess risk to individuals

Notify the ICO within 72 hours where required (we may submit details in phases)

Notify affected individuals where the risk is high

Record all incidents in the breach register and capture lessons learned

15. Training, Monitoring and Audit

Mandatory data protection training for all staff (on induction and annually)

Spot checks and internal audits of compliance and records

Supplier monitoring against contractual obligations

16. Contact and Complaints

For questions, rights requests or concerns, contact the Data Protection Lead at [insert email/phone].

Individuals may also complain to the Information Commissioner's Office (ICO): https://ico.org.uk/

17. Review

Updated and Reviewed: 29 September 2025

Next review due: 29 September 2026

This policy will be reviewed at least annually or sooner if law/guidance changes.