Telford Court

UK GDPR Policy and Procedure

2026-2027

Contents

1. Policy Statement

The Greenhouse is committed to ensuring the privacy and security of all personal data it holds about staff, learners, parents/carers and other individuals. This policy sets out how The Greenhouse meets its obligations under UK GDPR and the Data Protection Act 2018, and ensures that personal data is collected, used and protected lawfully, fairly and transparently.

This policy applies to all Greenhouse staff, including volunteers and contractors, and covers all personal data processed in connection with the work of The Greenhouse.

The Greenhouse adheres to the seven key principles of UK GDPR:

- Lawful, fair and transparent
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

2. Legal Framework

This policy complies with:

- UK GDPR (as defined in section 3(11) of the Data Protection Act 2018)
- The Data Protection Act 2018
- The Data Use and Access Act 2025
- Keeping Children Safe in Education 2026
- General Regulations for Approved Centres (JCQ)

3. Roles and Responsibilities

Data Protection Officer (Jon Simpson)

- Holds day-to-day responsibility for UK GDPR compliance across The Greenhouse
- Acts as first point of contact for data subjects and the ICO
- Manages Subject Access Requests and data breach responses
- Delivers, records and monitors data protection training
- Maintains the Record of Processing Activities (ROPA)

Head of Education (Fiona Conde)

- Holds strategic accountability for data protection compliance
- Makes the final decision on whether to notify the ICO following a data breach, in consultation with the DPO
- Approves this policy and ensures it is kept up to date
- Chairs annual data protection review

Senior Leadership Team

- Supports the DPO and Head of Education in implementing this policy
- Ensures sufficient resources are allocated to data protection
- Promotes a culture of privacy by design

Designated Safeguarding Lead (DSL)

- Ensures safeguarding referrals are made promptly, overriding confidentiality considerations where required
- Liaises with the DPO on data sharing decisions in safeguarding contexts

All Staff

- Process personal data only as required for their role
- Keep personal data secure and report any breach or near-miss to the DPO immediately
- Complete mandatory data protection training
- Follow all Greenhouse data protection policies and procedures

4. Data Held by The Greenhouse: Purpose, Legal Basis and Retention

The Greenhouse processes personal data across several categories. The table below sets out what data is held, why, the legal basis and how long it is retained. Full details are in the Data Security and Retention Policy.

Data Category	Data Held	Purpose / Legal Basis	Retention Period
Learner Data	Name, DOB, contact details, NI number, prior qualifications, attendance, progress records	Contractual obligation and legal compliance (UK GDPR Art. 6(1)(b) & (c))	6 years post programme end
Special Category Data	Health information, SEND needs, ethnicity (where disclosed)	Substantial public interest / explicit consent (Art. 9(2)(g) & (a))	6 years post programme end
Staff Data	HR records, payroll, DBS, performance and training records	Contractual and legal obligation (Art. 6(1)(b) & (c))	6 years post employment end
Safeguarding Records	Disclosures, risk assessments, multi-agency referrals	Legal obligation and vital interests (Art. 6(1)(c) & (d))	Until learner's 25th birthday (or longer if directed)
Employer / Partner Data	Contact details, organisation name, placement records	Legitimate interests (Art. 6(1)(f))	3 years post contract end
Website / Enquiry Data	Name, email, enquiry details	Consent (Art. 6(1)(a))	12 months or until consent withdrawn

Where data is special category data (health, ethnicity, religion, sexual orientation etc.), The Greenhouse applies additional safeguards including restricted access and encryption.

5. Subject Access Requests (SARs)

Any individual has the right to request access to the personal data The Greenhouse holds about them. This is a Subject Access Request (SAR).

The One-Month Rule

The Greenhouse must respond to a SAR within one calendar month of receipt. Where a request is complex or numerous, this can be extended by a further two months. The individual must be notified of any extension within the first month. Responses are provided free of charge unless the request is manifestly unfounded or excessive.

SAR Process

- Any member of staff who receives a SAR (written, verbal or electronic) must log it immediately and notify the DPO. The one-month clock starts from the date of receipt.
- Before releasing any data, the identity of the requestor must be verified. If the request is made on behalf of another person, authority to act must be confirmed.
- The DPO coordinates a search of all relevant systems (learner management system, email, paper files) for personal data relating to the requestor.
- Data must be reviewed and third-party information redacted before release. Exemptions (e.g. safeguarding, legal proceedings) must be considered.
- The individual receives a copy of their personal data together with a covering letter within one month of the request. The response is logged.

A SAR response template is available from the DPO. Staff must not attempt to respond to a SAR without DPO guidance.

6. Personal Data Breach: Reporting and Escalation

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Examples include:

- Sending an email containing personal data to the wrong recipient
- Loss or theft of a device, USB stick or paper records containing personal data
- Unauthorised access to learner or staff records
- Ransomware or cyber-attack affecting personal data systems
- Disclosing information about a learner to an unauthorised third party

The 72-Hour Reporting Requirement

The Greenhouse has 72 hours from becoming aware of a personal data breach to report it to the Information Commissioner's Office (ICO) — if the breach is likely to result in a risk to individuals' rights and freedoms. The DPO must be notified immediately upon any suspected breach being identified. Not all breaches require ICO notification, but all breaches must be documented internally.

Breach Reporting Process

- Identify and contain: Any staff member who discovers a breach must stop it where possible and report immediately to their line manager and the DPO. Do not investigate independently.
- Notify the DPO immediately: The DPO logs the breach, assesses risk and initiates internal escalation. All communications are time-stamped.
- Internal escalation: The DPO escalates to the Head of Education and SLT within 24 hours of awareness. SLT reviews severity and determines next steps.
- Risk assessment: The DPO and SLT assess the type and volume of data involved, likely impact on individuals, and whether reporting to the ICO is required.
- Decision to report to ICO: The Head of Education, in consultation with the DPO and SLT, decides whether to notify the ICO. If there is any doubt, the presumption is to report within 72 hours.
- Notify affected individuals: If the breach poses a high risk to individuals, affected data subjects must be notified without undue delay. The DPO drafts the notification with SLT approval.

- Document and review: All breaches are recorded in the Breach Log. A post-breach review is conducted to identify lessons learned and any changes needed.

Report to ICO (within 72 hours)	Document Internally Only
Breach likely to risk individuals' rights and freedoms **Large volume of data involved** **Special category data compromised** **Financial data or credentials exposed**	Accidental internal disclosure quickly remedied Small volume of non-sensitive data affected No likely risk to individuals Immediate containment confirmed

7. Training Expectations

All staff are required to complete data protection training. This is a mandatory condition of employment at The Greenhouse.

Mandatory Induction Training

All new staff must complete UK GDPR induction training before or on their first working day, and in any event no later than within the first two weeks of employment. Induction training covers:

- The key principles of UK GDPR and The Greenhouse's legal obligations
- What constitutes personal data and special category data
- Staff responsibilities for keeping data secure
- How to recognise and report a data breach
- How to handle a Subject Access Request
- Data sharing rules, including safeguarding considerations

Annual Refresher Training

All staff must complete a refresher training session at least once per year. Refreshers are scheduled as part of the staff training calendar and attendance is mandatory. Training is updated to reflect changes in legislation, ICO guidance and lessons learned from any incidents during the year.

Role-Specific Training

Staff with enhanced data responsibilities (including the DPO, Head of Education and those managing learner records) receive additional training relevant to their role. This may include specialist training on safeguarding and data sharing, SAR handling or DPIA completion.

Recording and Monitoring

Completion of all data protection training is recorded on the staff training log. Line managers are responsible for ensuring direct reports complete required training. Non-completion of mandatory training is addressed through the standard performance management process.

8. Data Sharing

General Principle

The Greenhouse only shares personal data with third parties where there is a lawful basis for doing so, the sharing is proportionate, and the recipient handles data appropriately. All data sharing arrangements with third parties should be governed by a Data Sharing Agreement or Data Processing Agreement as appropriate.

Sharing with Referring Schools and Local Authorities

The Greenhouse regularly receives referrals from schools and local authorities (LAs) and may be required to share information about learner progress, attendance and outcomes with those bodies. Where this occurs:

- The legal basis for sharing is typically legal obligation (Art. 6(1)(c)) or legitimate interests (Art. 6(1)(f))
- Learners (and parents/carers where appropriate) are informed that data will be shared with the referring body
- Only the minimum necessary data is shared — sharing must be proportionate to the purpose
- Shared data is transmitted securely (e.g. encrypted email or secure portal) and never via personal email accounts or unencrypted devices

Safeguarding Takes Priority Over Confidentiality

Where there is a safeguarding concern, the duty to protect a child or vulnerable adult takes priority over any duty of confidentiality. Staff must not allow data protection considerations to prevent or delay a safeguarding disclosure or referral.

If a learner discloses information that gives rise to a safeguarding concern, that information must be shared with the Designated Safeguarding Lead (DSL) immediately, regardless of any expectation of confidentiality. The DSL will determine whether to refer to children's services, the police or other agencies. Data protection law does not prevent such referrals — Article 9(2)(g) of UK GDPR provides a lawful basis for processing special category data in the substantial public interest, including child protection. Where a referral is made, the threshold for sharing is low: if in doubt, share.

Multi-Agency Working

Where The Greenhouse is engaged in multi-agency working (e.g. EHCP processes, Youth Offending Team involvement or Local Authority support plans), it follows any applicable information sharing protocols. In the absence of a formal protocol, sharing decisions are made on a case-by-case basis with DPO input.

9. Rights of Data Subjects

Under UK GDPR, individuals have the following rights. Not all rights apply in all circumstances. Staff should direct any request to the DPO immediately.

Right	Summary
Right of Access (SAR)	Receive a copy of personal data held within one month (see Section 5).
Right to Rectification	Have inaccurate personal data corrected without undue delay.
Right to Erasure	Request deletion of personal data in certain circumstances, subject to legal retention obligations.
Right to Restriction	Request that processing of their data is restricted in certain circumstances.
Right to Data Portability	Receive personal data in a commonly used format where consent is the legal basis.
Right to Object	Object to processing based on legitimate interests or for direct marketing purposes.
Rights re Automated Decisions	Not be subject to a decision based solely on automated processing that produces significant effects.

10. Monitoring and Review

This policy is reviewed annually by the Head of Education and DPO, or following any significant data protection incident, regulatory change or ICO guidance update. Compliance is monitored through:

- Training completion records
- Annual data protection audit
- Review of the Breach Log and SAR log
- DPO reports to SLT
- Self-assessment against the ICO Accountability Framework

Failure by staff to comply with this policy may result in disciplinary action up to and including dismissal. Organisational non-compliance may result in ICO enforcement action and financial penalties of up to £17.5 million or 4% of worldwide turnover.

11. Related Policies

This policy must be read in conjunction with the following related policies:

- Safeguarding and Child Protection Policy
- Breach Notification Policy and Procedure
- Subject Access Request Policy and Procedure
- Archiving, Disposal and Storage of Records Policy

This policy has been written by Fiona Conde (Headteacher) and approved by Jon Simpson (Business Director).

Approval Date: June 2026

Review Date: June 2027