Telford Court

Archiving, Disposal and Storage of Records Policy

2026-2027

Contents

1. Policy Statement

The Greenhouse is committed to managing all records — whether held in paper or digital format — in a secure, organised and lawful manner throughout their lifecycle. This includes how records are created, stored, archived and ultimately disposed of.

This policy ensures that:

- Records are kept securely and are accessible only to those with a legitimate need
- Personal data is not retained longer than necessary
- Records are archived in a way that preserves their integrity
- Confidential records are disposed of safely and without risk of breach
- The Greenhouse meets its legal obligations under UK GDPR, the Data Protection Act 2018 and relevant sector-specific guidance

2. Legal Framework

This policy complies with:

- UK GDPR and the Data Protection Act 2018
- The Data Use and Access Act 2025
- The UK Government Records Management Code of Practice 2021
- Keeping Children Safe in Education 2026
- Limitation Act 1980 (which governs retention periods for legal claims)
- HM Revenue and Customs requirements for financial records

3. Roles and Responsibilities

Data Protection Officer (Jon Simpson)

- Holds overall responsibility for records management compliance
- Maintains and reviews the retention schedule
- Advises staff on correct storage, archiving and disposal procedures
- Oversees the secure disposal of confidential records

Head of Education (Fiona Conde)

- Ensures sufficient systems and resources are in place for secure records management
- Approves this policy annually

All Staff

- Store records in the correct location (physical or digital) as set out in this policy
- Do not retain personal data beyond its specified retention period
- Do not dispose of records without following the correct procedure
- Report any loss, damage or suspected breach involving records to the DPO immediately

4. Principles of Records Management

The Greenhouse applies the following principles to all records it holds:

Principle	What This Means in Practice
Necessary	Only records required for a legitimate purpose are created and retained.
Accurate	Records are kept up to date. Inaccuracies are corrected promptly.
Secure	Records are protected from unauthorised access, loss, theft or damage — whether held in paper or digital format.
Accessible	Records can be located and retrieved in a timely manner by authorised staff.
Retained Appropriately	Records are kept for the period specified in the retention schedule and no longer.
Disposed of Safely	When retention periods expire, records are disposed of securely and in a way that prevents reconstruction of personal data.

5. Storage of Records

Digital Records

Digital records must be stored on approved Greenhouse systems only. Staff must not store personal data on personal devices, personal cloud accounts or unencrypted USB drives.

- Learner and staff records are held on the Greenhouse's management information system
- Documents containing personal data must be saved to secure shared drives with appropriate access controls
- Email containing personal data must not be forwarded to personal email accounts
- Where data is shared externally, this must be via encrypted email or a secure portal
- All devices used to access personal data must be password protected and encrypted

Physical Records

Paper records containing personal or confidential information must be stored securely at all times.

- Confidential paper records are stored in locked filing cabinets
- Access to filing cabinets is restricted to authorised staff only
- Paper records must not be left unattended in communal areas
- Records containing personal data must not be taken off-site without authorisation from the DPO
- When not in use, physical records must be returned to secure storage immediately

Safeguarding Records

Safeguarding records are treated with the highest level of confidentiality and are stored separately from general learner files. Access is restricted to the Designated Safeguarding Lead and the Head of Education. Safeguarding records are never disposed of without specific authorisation from the DPO and Head of Education.

6. Retention Schedule

Personal data must not be kept longer than necessary. The table below sets out the key retention periods applied by The Greenhouse. A full retention schedule is maintained by the DPO.

Record Category	Examples	Retention Period	Trigger for Deletion
Learner Records	Enrolment forms, progress records, attendance, qualifications	6 years after programme end	Date of last programme activity
Safeguarding Records	Disclosures, referrals, risk assessments, case notes	Until the learner's 25th birthday (minimum), or longer if directed by statutory agencies	Learner's date of birth
Staff Records	Contracts, payroll, DBS, appraisals, training records	6 years after employment ends	Date employment ended
Financial Records	Invoices, payroll records, funding claims, expenses	7 years after the end of the financial year	Financial year end
Health and Safety Records	Accident and incident logs, first aid records	3 years (or until the individual turns 18 if a minor)	Date of incident
Complaints Records	Formal complaints, outcomes and correspondence	3 years after resolution	Date complaint closed
Employer and Partner Data	Placement records, contact details, agreements	3 years after contract or placement end	Date contract ended

Record Category	Examples	Retention Period	Trigger for Deletion
CCTV Footage	Where held on Greenhouse premises	31 days unless subject to an investigation	Date of recording
Website Enquiries	Contact form submissions, email enquiries	12 months or until consent withdrawn	Date of submission

Where a legal claim is anticipated or active, relevant records must be retained for the duration of the claim, regardless of the standard retention period. The DPO must be notified in such cases.

7. Archiving

Archiving refers to the transfer of records that are no longer in active use but must be retained for compliance, legal or historical purposes. Archived records are not deleted but are moved to secure, lower-access storage.

Digital Archiving

- Records due for archiving are moved to a designated archive folder on the Greenhouse shared drive or management information system
- Archived records are read-only and cannot be edited
- Access to archived records is restricted to the DPO and Head of Education
- The DPO reviews archived records annually against the retention schedule to identify records due for disposal

Physical Archiving

- Paper records no longer in active use are placed in clearly labelled archive boxes, identified by record type and the date the retention period expires
- Archive boxes are stored in a locked, secure location within Greenhouse premises
- A log of archived physical records is maintained by the DPO
- Physical archive records are not removed from secure storage without DPO authorisation

8. Disposal and Destruction of Records

When a record reaches the end of its retention period, it must be disposed of securely. The method of disposal depends on the nature of the record.

Paper Records

- All confidential paper records must be shredded using a cross-cut or micro-cut shredder — strip-cut shredders must not be used for personal data
- Where shredding is carried out by a third-party contractor, a certificate of destruction must be obtained and retained for 3 years
- Paper records must never be disposed of in general waste or recycling bins

Digital Records

- Deleting a file does not constitute secure disposal — digital records must be permanently deleted and removed from all backups and recycle bins
- Where devices are decommissioned, data must be wiped using an approved method (e.g. secure overwrite software) or the device physically destroyed
- Cloud-based records must be deleted in line with the provider's secure deletion procedures
- The DPO must confirm that deletion from cloud or third-party systems has been completed

Disposal Log

The DPO maintains a disposal log recording:

- The type and description of records disposed of
- The date of disposal
- The method of disposal
- The name of the member of staff who authorised and carried out the disposal

No records containing personal data may be disposed of without authorisation from the DPO.

9. Data Breaches Involving Physical Records

The loss, theft or unauthorised disclosure of physical records containing personal data constitutes a personal data breach and must be reported to the DPO immediately. This includes:

- Loss or theft of paper files or archive boxes
- Incorrectly addressed post containing personal data
- Unauthorised access to locked filing cabinets
- Records found in communal or unsecured areas

All such incidents are handled in line with the Greenhouse's UK GDPR Policy and Procedure, including the 72-hour ICO notification requirement where applicable.

10. Monitoring and Review

This policy is reviewed annually by the DPO and Head of Education, or following any significant incident relating to records management. Compliance is monitored through:

- Annual audit of physical and digital storage arrangements
- Review of the disposal log
- DPO spot-checks on record storage and access controls
- Staff training records confirming awareness of records management obligations

Failure by staff to comply with this policy may result in disciplinary action up to and including dismissal. Significant breaches may also trigger ICO investigation and enforcement action.

11. Related Policies

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

- UK GDPR Policy and Procedure
- Breach Notification Policy and Procedure
- Subject Access Request Policy and Procedure
- Safeguarding and Child Protection Policy

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

Approval Date: June 2026

Review Date: June 2027