STAFFPOWER GROUP

RECRUITMENT & TRAINING

Document Retention & Secure Storage Policy

| Version 1.0 |

Policy Commencement Date	08/12/2025
Policy Version	1.0
Review by	07/12/2026
Document Controller	Robert Longstaff
Signature	*R. Longstaff*

Contents page

1. Introduction

The purpose of this policy is to ensure that Staff Power Training (SPT) manages, retains, and disposes of all records (paper and electronic) in a manner that is secure, efficient, and compliant with UK legislation including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and requirements set by funding bodies and Awarding Organisations.

2. Scope

This policy applies to all employees, contractors, and third parties who have access to information held by SPT. It covers all records created or received in the course of business, regardless of format (e.g., email, paper files, databases, audio recordings).

3. Guiding Principles

We adhere to the following principles regarding data retention:

- **Storage Limitation**: Data will not be kept for longer than is necessary for the purpose for which it was processed.
- **Security**: Records will be stored securely to prevent unauthorised access, accidental loss, or damage.
- **Integrity**: Records will be maintained in a way that ensures they remain complete, accurate, and legible.

4. Secure Storage Protocols

4.1. Physical Records (Paper)

- *Active Files: Must be stored in lockable filing cabinets or secure storage rooms when not in use. Keys must be held only by authorised staff.*
- *Clean Desk Policy: No sensitive documentation (learner forms, HR records) should be left on desks when unattended.*
- *Transport: Physical records should not be removed from the premises unless absolutely necessary (e.g., for an external audit). If removed, they must be carried in a locked case and never left in a vehicle overnight.*

4.2. Digital Records

- *Access Control: Access to digital folders is restricted by role (Role-Based Access Control). Only staff who need access to learner or financial data for their job will have it.*
- *Encryption: All laptops and portable devices (USBs) used by staff must be encrypted.*
- *Servers/Cloud: Data must be stored on secure servers located within the UK or EEA, or with a provider compliant with UK GDPR (e.g., via Standard Contractual Clauses).*
- *Backups: Regular automated backups are performed to protect against data loss (e.g., ransomware or hardware failure).*

5. Retention Schedule

The table below outlines the statutory and regulatory retention periods for specific categories of documents.

A. Learner & Funding Records

Document Type	Retention Period	Reason / Authority
Learner Files *(Enrolment forms, ILR data, Learning Agreements, reviews)*	6 years from the end of the financial year in which the last payment was made.	ESFA Funding Rules *(Limitation Act 1980)*
All Awarding Organisations related paperwork	ABBE – 3 years ETA – 3 years NCFE – 3 years QNUK – 3 years CITB – 3 years	Awarding Organisation Requirements
Safeguarding Concerns	10 years from the date of the last entry or concern.	Best Practice / Care Act

B. Corporate & Financial Records

Document Type	Retention Period	Reason / Authority
Annual Accounts / Budgets	6 years + current financial year.	Companies Act 2006
Invoices / Bank Statements	6 years + current financial year.	HMRC *(Tax purposes)*
Payroll Records	3 years minimum *(6 recommended)*.	HMRC / PAYE Regulations
Insurance Policies	Permanently *(or 40 years for Employers' Liability)*.	Liability claims can be retroactive
Contracts with Suppliers	6 years after contract expiry.	Limitation Act 1980

C. Human Resources (Staff)

Document Type	Retention Period	Reason / Authority
Personnel Files *(Ex-Employees)*	6 years after employment ceases.	Limitation Act *(Contract claims)*
Recruitment *(Unsuccessful)*	6 months to 1 year after the interview.	Time limit for discrimination claims
DBS Check Outcomes	Current + duration of employment.	DBS Code of Practice
Disciplinary Records	6 - 12 months for warnings *(depending on severity)*.	ACAS Code of Practice

D. Health & Safety

Document Type	Retention Period	Reason / Authority
Accident Book	3 years from the date of entry.	RIDDOR / Limitation Act
Risk Assessments	Current + 3 years.	Health & Safety at Work Act
Personnel Files *(Ex-Employees)*	6 years after employment ceases.	Limitation Act *(Contract claims)*

6. **Disposal and Destruction**
   When a document reaches the end of its retention period, it must be disposed of securely. It is a breach of this policy to place personal data in general waste bins.
   - **Paper**: Must be shredded using a cross-cut shredder or placed in confidential waste consoles collected by a certified disposal company *(ISO 15489 compliant)*. A Certificate of Destruction must be obtained for bulk disposal.
   - **Digital**: Files must be permanently deleted. For decommissioned hardware *(laptops, hard drives)*, physical destruction or professional data wiping is required.

7. **Archiving vs. Live Data**
   - **Live Data**: Records currently in use for active learners or the current financial year. Kept in immediate access folders/cabinets.
   - **Archived Data**: Records that are closed but must be kept for legal reasons *(e.g., a learner who finished 2 years ago)*. These should be moved to a separate "Archive" secure folder *(digital)* or deep storage *(physical)* to prevent clutter and accidental alteration.

8. **Data Breaches**
   If a document is lost, stolen, or securely retained past its legal limit without justification, this constitutes a data breach. All breaches must be reported immediately to the Data Protection Officer.

9. **Policy Review**
   This policy will be reviewed annually, or more frequently if there are significant changes in legislation, working practices, or following any related incidents.