ESTAR

ELITE SKILLS, TRAINING & RECRUITMENT

CP-006

Document Retention and Secure Storage Policy

REV: 00

Policy owner: Head of Quality & Compliance / Data Protection Officer (DPO)
Applies to: All staff, associates, subcontractors and partners handling ESTAR records
Provision: Funded and non-funded delivery (including apprenticeships and adult skills)
Review cycle: Annual, or following changes to legislation, funding or inspection requirements
Version: 00

---

1. Purpose

ESTAR Education is committed to managing information responsibly. This policy sets out how documents and records are **retained, stored, protected and securely disposed of** to ensure:

- compliance with data protection legislation;
- ESFA, awarding organisation and audit requirements;
- protection of personal, confidential and sensitive information; and
- availability of records for inspection, audit and quality assurance.

---

2. Scope

This policy applies to all records created, received or maintained by ESTAR, including:

- learner, apprentice and employer records;
- assessment, IQA and EPA-related evidence;
- safeguarding and welfare records;
- funding, finance and audit documentation;
- staff and HR records;
- governance and quality assurance records;
- electronic and paper-based documents.

---

3. Principles

ESTAR will ensure that records are:

- **Lawfully retained** – only for as long as necessary and required;
- **Securely stored** – protected against unauthorised access, loss or damage;
- **Accurate and complete** – suitable for audit and inspection;
- **Accessible** – retrievable when legitimately required; and
- **Securely disposed of** – once retention periods expire.

4. Roles and responsibilities

4.1 Head of Quality & Compliance / DPO

- Oversees retention and secure storage arrangements.
- Approves retention schedules and disposal actions.
- Ensures compliance with UK GDPR and funding requirements.

4.2 Senior Leadership Team

- Ensures adequate systems and resources for secure storage.
- Provides oversight of high-risk or sensitive records.

4.3 All staff and associates

- Create, store and handle records in line with this policy.
- Protect information from unauthorised access.
- Report any loss, breach or misuse of records immediately.

5. Record categories

Records covered by this policy include (but are not limited to):

- **Learner records:** enrolment, eligibility, attendance, progress, assessment and achievement.
- **Assessment records:** assessment plans, evidence, feedback, IQA sampling, standardisation records.
- **Safeguarding records:** concerns, referrals and actions (held separately with restricted access).
- **Funding and finance records:** ILR data, claims, evidence packs, audit files.
- **Staff records:** contracts, DBS checks, training and disciplinary records.
- **Governance records:** policies, minutes, quality reviews and improvement plans.

6. Retention periods

ESTAR retains records in line with:

- statutory requirements;
- ESFA funding rules and audit expectations;
- awarding organisation and EPAO requirements; and
- business and quality assurance needs.

Typical retention examples (indicative)

- **Learner/apprentice records:** minimum of **6 years** after completion/withdrawal
- **Assessment and IQA records: 6 years** after certification
- **Funding and audit records: 6 years** (or longer if contractually required)
- **Safeguarding records:** retained in line with statutory safeguarding guidance
- **Staff employment records: 6 years** after employment ends (unless otherwise required)

Exact retention periods are detailed in ESTAR's Retention Schedule.

---

7. Secure storage – electronic records

Electronic records must be:

- stored on approved, secure systems (e.g. controlled cloud platforms);
- protected by role-based access and strong passwords;
- backed up regularly;
- accessed only by authorised users.

Portable devices containing personal data must be encrypted where possible and protected against loss or theft.

---

8. Secure storage – paper records

Paper records must be:

- stored in locked cabinets or secure rooms;
- accessible only to authorised staff;
- transported securely when moved off-site;
- protected from damage (fire, water, unauthorised removal).

Safeguarding and highly sensitive records must be stored separately with enhanced access controls.

---

9. Access control and confidentiality

Access to records is granted on a **need-to-know basis** only. Staff must not:

- access records unnecessarily;
- share information without authority; or
- remove records from secure storage without permission.

Breach of confidentiality may result in disciplinary action.

---

10. Secure disposal of records

When records reach the end of their retention period, they must be disposed of securely:

- **Paper records:** cross-cut shredding or approved confidential waste services.
- **Electronic records:** secure deletion in line with IT procedures.
- **Devices/media:** wiped or destroyed using approved methods.

Disposal actions may be logged where required for audit purposes.

---

11. Data breaches and incidents

Loss, theft or unauthorised access to records must be reported immediately in line with ESTAR's **Data Protection Policy**.

ESTAR will:

- investigate incidents promptly;
- mitigate risk;
- notify the ICO where legally required; and
- take corrective action to prevent recurrence.

---

12. Training and awareness

- Staff receive training on information handling and secure storage.
- This policy forms part of induction and ongoing compliance training.

---

13. Monitoring and review

Compliance with this policy is monitored through:

- internal audits;
- quality assurance activity;
- inspection and funding audits.

This policy is reviewed:

- annually; and

- following changes to legislation, funding rules or operational risk.

Date of last Review	Print Name	Position
02/02/2026	Keiran Casey	Chief Executive Officer
	Darren Beach	Quality Manager