Document Retention Policy

East Birmingham Community Forum (EBCF)

Version:	**v5.0**
Date Issued:	**January 2026**
Review Date:	**January 2027**

Document Control

Policy Owner: Human Resources

Approved By: Head of Quality

Contents

1. Aim

The aim of this policy is to provide clear guidance on the secure storage, retention, and disposal of all records created or received by EBCF. This includes, but is not limited to, records relating to:

- Training and learner portfolio evidence
- Government or externally funded contract delivery (commissioned services)
- General business operations and administration

This policy ensures that:

- Records are retained for the correct duration in line with legal and contractual obligations.
- Storage methods maintain quality, accessibility, and confidentiality.
- Disposal is secure, compliant, and documented.
- All activity aligns with the Data Protection Act 2018, UK GDPR, the Freedom of Information Act 2000, and any relevant funding or commissioning body requirements.

EBCF is committed to maintaining robust document management practices to ensure compliance, accountability, and effective operational delivery.

2. Scope

This policy applies to:

- All employees of EBCF, regardless of role or contract type.
- Partners, contractors, or third parties processing records on behalf of EBCF.
- All records, whether physical or digital, created during:
    - Training provision ○ Commissioned or funded service delivery ○ Internal operations and governance

This policy applies across all EBCF sites and systems, including remote working environments and cloud-based storage platforms.

3. Policy Requirements

3.1. Record Types

This policy covers, but is not limited to:

- Learner portfolios and assessment records.
- Client registration, eligibility, and consent documentation.
- Service delivery records, action plans, and progress reviews.
- Outcome evidence and contractual performance monitoring documents.
- Board reports, financial records, and HR files.
- Contracts of employment, lease agreements, and operational documentation.

All records must be clearly categorised and maintained in a structured format to support accessibility and audit requirements.

3.2. Storage Standards

- Records must be stored in a format that preserves their integrity, readability, and accessibility for the required retention period.
- Physical records must be held in secure, access-controlled locations protected from environmental damage.
- Digital records must be stored in secure systems with appropriate access controls, encryption, and audit trails.
- Back-up systems must be in place for digital records to ensure recoverability in case of data loss.

Regular checks should be carried out to ensure that storage systems remain secure, accessible, and fit for purpose.

3.3. Security and Access Control

- Access to records is restricted to authorised personnel only, based on role requirements.
- Confidential information must be secured in locked storage or password-protected/encrypted systems.
- All staff must complete annual data protection and confidentiality training.

Any unauthorised access, data breach, or suspected risk must be reported immediately in line with EBCF's data protection procedures.

3.4. Retention Periods

Retention periods will comply with legal, operational, and contractual requirements. Examples include:

- Board Reports – 6 years
- Financial Records – 6 years (or as required by HMRC)
- HR Records – Duration of employment + 6 years
- Client/Service Delivery Records – As specified in the relevant funding or commissioning agreement (minimum 6 years after service completion unless otherwise required)
- Learner Assessment Records – 3 years after certification

Duplicate records should be avoided unless operationally necessary.

Retention schedules will be reviewed periodically to ensure alignment with current legal and contractual requirements.

3.5. Disposal of Records

- Physical records containing personal or confidential data must be destroyed using an approved confidential waste disposal service, with a certificate of destruction retained.
- Digital records must be securely deleted so they cannot be reconstructed.
- Disposal must be logged, recording the date, method, and authorisation.
- No destruction of commissioned service records may occur before the contractual retention period ends, without senior management approval.

All disposal activity must be authorised and auditable to ensure compliance and accountability.

4. Learner, Client, and Commissioned Service Records

4.1. Learner Portfolio Return Policy

- Learners may request the return of their portfolio of evidence in writing within 2 weeks after completion of their programme.
- All learner portfolios must be held at Head Office until the relevant quality assurance visit has taken place.
- Assessment records (marking criteria, reports, task sheets, risk assessments, learner feedback, IQA documentation) must be retained for 3 years after certification.

4.2. Client Records for Commissioned Services

- All client records relating to funded or commissioned services must be accurate, up-to-date, and filed in the approved storage system.
- Records must meet the quality, evidence, and audit requirements set out in the relevant funding agreement.

4.3. Subject Access Requests (SARs)

- Individuals have the right to access and receive copies of their personal data.
- Requests can be made verbally, in writing, or via social media.
- SARs will be acknowledged within 5 working days and responded to within 1 month (extended by up to 2 months for complex cases).
- Identity verification is required before releasing personal data.
- Where records are part of commissioned services, responses will be managed in line with both legal and contractual obligations.

5. Roles and Responsibilities

- Data Protection Officer (DPO): Oversees compliance with data protection law, approves SAR responses, and advises on secure record handling.
- Managers: Ensure their teams comply with retention schedules, storage standards, and contractual obligations.
- Compliance Officer: Monitors record-keeping practices for funded/commissioned service delivery and coordinates audit preparation.
- Staff Members: Follow the policy, maintain accurate records, and report breaches or risks promptly.

All staff share responsibility for maintaining accurate, secure, and compliant records within their roles.

6. Review Process

- This policy will be reviewed annually, or sooner if there are changes in legislation, operational requirements, or the terms of a funded/commissioned service agreement.

Findings from audits, inspections, or incidents will be used to inform updates to this policy.

7. Version Control

Version	Description of Change	Author	Date	Approved by
1.0	Version 1;0	S.Khan / / Z. Sharif	July 2023	
2.0	Version 2.0	S.Khan / J.Hall	July 2024	
3.0	Version 3.0	S.Khan /J.Hall	January 2025	
4.0	Version 4.0 Policy updated to strengthen document retention processes, with additional guidance on storage, security, monitoring, and compliance	S.Khan (HR)	January 2026	S.Etheridge (Head of Quality)