DATA PROTECTION AND DATA RETENTION POLICY

Policy Review Date: 1 April 2026
Next Review Date: 1 April 2027

1. Purpose

This policy establishes a comprehensive framework for the collection, processing, storage, retention, and disposal of data within Footprint School of Business (FSOB). It ensures that all data is managed securely, lawfully, and transparently in compliance with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Ofqual General Conditions of Recognition
- NCFE requirements for learner data, assessment records, and certification

The policy aims to:

- Protect the confidentiality, integrity, and availability of data
- Ensure compliance with legal and regulatory obligations
- Provide clear procedures for data lifecycle management
- Support audit and evidence requirements for EQA

2. Scope

This policy applies to all data processed by FSOB, including:

- Learner records (enrolment, ILPs, assessments, portfolios, certification data)
- Staff records (HR, payroll, contracts, CPD records)
- Financial and contractual records
- Communication records (emails, reports, correspondence)
- Data stored in both digital and physical formats

This policy applies to all staff, contractors, and third parties handling FSOB data.

3. Key Data Protection Principles (UK GDPR)

FSOB adheres to the following principles:

1. **Lawfulness, Fairness, and Transparency**
   Data is processed lawfully and transparently
2. **Purpose Limitation**
   Data is collected for specified and legitimate purposes
3. **Data Minimisation**
   Only necessary data is collected
4. **Accuracy**
   Data is kept accurate and up to date
5. **Storage Limitation**
   Data is retained only as long as necessary
6. **Integrity and Confidentiality**
   Data is protected against unauthorised access or loss
7. **Accountability**
   FSOB demonstrates compliance through documentation and audit trails

4. Lawful Basis for Processing

FSOB processes personal data under the following lawful bases:

- **Legal Obligation:**
  Compliance with awarding body requirements (e.g. NCFE registration and certification)
- **Contract:**
  Delivery of education and training services
- **Legitimate Interests:**
  Quality assurance, monitoring, and improvement
- **Consent (where applicable):**
  For specific uses such as marketing or recordings

5. Data Subject Rights

Learners and staff have the right to:

- Access their personal data (Subject Access Request)

- Request rectification of inaccurate data
- Request erasure (where legally permissible)
- Restrict or object to processing
- Request data portability

All requests are processed within statutory timelines (normally one month).

6. Data Retention Periods

Retention periods are aligned with regulatory and awarding body requirements:

Data Type	Retention Period	Rationale
Learner assessment records & portfolios	Minimum **3 years after certification**	Required for EQA and audit
Learner registration data	3 years	Awarding body verification
ILPs, progress reviews	Duration of course + 3 years	Quality assurance evidence
Certification records	Permanent (or as per awarding body)	Verification purposes
Financial records	7 years	Legal and tax compliance
Staff records	6 years after employment ends	Employment law
Complaints and appeals records	3 years	Audit and compliance
Safeguarding records	As per safeguarding policy (often longer)	Legal obligation

Important Improvement:
Your original policy deletes portfolios within 14 days — this is not compliant with NCFE expectations. Evidence must be retained for EQA sampling.

7. Data Storage and Security

FSOB ensures that all data is securely stored through:

7.1 Digital Security

- Password-protected systems
- Secure cloud storage
- Role-based access controls
- Regular backups

7.2 Physical Security

- Locked storage for paper records
- Controlled access to premises

7.3 Access Control

- Data access limited to authorised personnel
- Access logs maintained

8. Data Archiving

Where data must be retained long-term:

- It is archived securely
- Access is restricted
- Data integrity is maintained
- Retrieval is possible for audit or EQA purposes

9. Data Disposal

When data reaches the end of its retention period:

Digital Data

- Permanently deleted from systems and backups

Physical Data

- Shredded or securely destroyed

All disposal actions are documented.

10. Data Breach Management

FSOB operates a structured breach management process:

10.1 Identification

- All suspected breaches reported immediately

10.2 Recording

- Logged in a **Data Breach Register**

10.3 Notification

- Serious breaches reported to ICO within **72 hours**

10.4 Investigation

- Root cause analysis conducted
- Corrective actions implemented

11. EQA and Audit Requirements

FSOB ensures availability of:

- Learner portfolios and assessment records
- Registration and certification data
- IQA and sampling documentation
- Audit trails of data access and changes

All records must be accessible during EQA visits.

12. Roles and Responsibilities

Senior Management:

- Overall accountability for compliance

Data Protection Lead / Compliance Officer:

- Monitor compliance
- Manage breaches and SARs

IT Manager:

- Ensure system security and backups

Staff:

- Handle data responsibly
- Report breaches immediately

13. Third-Party Data Processing

Where third parties process data:

- Data sharing agreements are in place
- GDPR compliance is ensured
- Data is only shared where necessary

14. Training and Awareness

- All staff receive **data protection training annually**
- Training includes:
    - GDPR principles
    - Data security
    - Handling sensitive information

15. Monitoring and Review

This policy is reviewed:

- Annually
- Following data breaches
- Following EQA feedback
- When legislation changes

16. Non-Compliance and Enforcement

Failure to comply with this policy may result in:

- Disciplinary action
- Legal consequences
- Reporting to regulatory bodies