Records Retention & Archiving Policy

March 2025
Doc Name: Records Retention & Archiving Policy
Doc Number: RRAP
Review Date: 03/2026

CIFA EDUCATION LTD registered at 94-96 Seymour Place, London, W1H 1NB.
Company Registration Number 14271739.

1: Introduction

CIFA Education Ltd is committed to managing records that are compliant with UK GDPR and other applicable regulations. This policy outlines how long different types of records are retained, the procedures for archiving and when records should be securely deleted or anonymised.

2: Purpose

The purpose of this policy is to:

- Ensure compliance with legal, regulatory and contractual obligations.
- Establish clear guidelines for the retention and disposal of records.
- Protect personal and confidential data by securely managing archived records.
- Maintain efficient storage and retrieval systems for essential documents.

3: Scope

This policy applies to all records held by CIFA Education Ltd, including those related to:

- Students and course participants
- Employees and contractors
- Financial transactions
- Compliance and regulatory reporting
- IT and security logs

4: Records Retention Schedule

Category	Retention Period	Reason for Retention
Student Records	7 years after course completion	Legal and regulatory requirements
Financial Records	6 years from the end of the financial year	HMRC and financial compliance
Employee Records	6 years post-employment	Legal and payroll obligations
Marketing Data	Until consent is withdrawn	GDPR consent-based processing. Please refer to **GDPR Policy Doc Ref: GDPR**
Customer Support Data	2 years after the last interaction	Service quality monitoring
Contracts & Agreements	6 years after contract termination	Legal obligations
Compliance Records	7 years (or longer if legally required)	Regulatory requirements. Refer to the **Organisational Policy for Handling Breaches & Monitoring Compliance. Doc Ref: OPHB.**
IT System Logs	12 months	Security monitoring and audits. **Refer to IT Security & Acceptable Use Policy, Doc Ref: ITSAP.**
Data Breach Reports	7 years	ICO reporting and audit requirements. **Refer to Data Breach Plan and Procedure, Doc Ref: DBPP**

5: Archiving Procedures

- Records that are no longer actively needed but must be retained for compliance will be securely archived.
- Archived records must be stored in encrypted and access-controlled environments.
- Only authorised personnel will have access to archived records.

6: Secure Disposal & Deletion

- At the end of the retention period, records will be securely deleted or anonymised.
- Physical documents will be shredded or incinerated.
- Digital records will be permanently deleted using secure erasure tools.

7: Responsibilities

- The **Compliance Officer** is responsible for overseeing records retention and archiving processes.
- Departmental leads are responsible for ensuring compliance with this policy within their areas of operation.

8: Policy Review

This policy will be reviewed annually or sooner if legal or operational changes require an update.