UK Professional Development Academy

Document Retention and Secure Storage Policy

Document Retention and Secure Storage Policy	Last Review:	January 2026
	Amended Date:	N/A
	Next planned review in 12 months, or sooner as required	

Document Retention and Secure Storage Policy

1. Introduction

UK Professional Development Academy manages records so that they remain accurate, accessible, secure and available for as long as there is a clear legal, regulatory, contractual or operational need. Personal data must not be retained indefinitely without justification.

2. Scope

This policy covers paper and electronic records relating to learners, assessment, quality assurance, certification, staff, finance, governance, complaints, safeguarding, contracts and business operations.

3. Core Principles

Records will be created and maintained accurately, classified by sensitivity, protected against unauthorised access, backed up where appropriate, retained according to an approved schedule and securely destroyed when no longer required. Legal holds, investigations or awarding organisation instructions may require longer retention.

4. Retention Schedule

The following periods are default minimums and may be extended where an awarding organisation, funder, contract, tax rule or legal matter requires it.

Record category	Default retention period
Learner enrolment and registration records	Six years after completion or withdrawal
Assessment *decisions, feedback and IQA records*	At least three years after certification, or longer if required by the awarding organisation
Certificate claim and achievement records	Indefinitely, or for the period required by the awarding organisation
Identity evidence	Only as long as necessary for verification and audit, normally no longer than six years after

	completion
Financial and tax records	Six years after the relevant accounting period
Staff personnel records	Six years after employment ends, subject to specific legal requirements
Complaints, appeals and malpractice cases	Six years after closure, or longer, where a continuing risk exists
Policies, governance minutes and key quality records	Current version plus at least six years of superseded records

5. Secure Storage

Electronic records will use access controls, strong passwords, encryption where appropriate, supported systems and reliable backups. Paper records containing personal or confidential information will be stored in locked cabinets or secure rooms. Access will be based on job role and reviewed periodically.

6. Sharing and Retrieval

Records may be shared only where there is a lawful and legitimate reason, including with awarding organisations, regulators, auditors, professional advisers or public authorities. Requests for access to personal data will be handled under the applicable data protection procedure.

7. Disposal

Paper records will be cross-cut, shredded, or destroyed by an approved confidential waste provider. Electronic records wilSecurityl be securely deleted from active systems and, where practicable, from backups in line with normal backup cycles. Storage devices must be securely wiped or destroyed before disposal.

8. Data Breaches and Incidents

Loss, unauthorised disclosure, corruption or destruction of records must be reported immediately to the designated data protection contact. Incidents will be contained, assessed, documented and

reported to the Information Commissioner's Office and affected individuals where legally required.

9. Responsibilities

The Data Protection Lead or nominated manager oversees the retention schedule. Record owners are responsible for accurate filing, restricted access and timely disposal. All staff must follow this policy and complete relevant training.

10. Monitoring and Review

Retention periods and security controls will be reviewed annually and whenever systems, contracts, legal duties or awarding organisation requirements change.