

DATA RETENTION POLICY

1. About this Policy

This Retention Policy outlines the retention, storage, and destruction periods for records held by CERT Solutions in compliance with relevant legal, regulatory, and operational requirements. It ensures that records are kept only for as long as necessary and that personal and sensitive data are handled securely and ethically.

2. Scope

This policy applies to all employees, contractors, and third-party processors who handle data on behalf of CERT Solutions including physical and digital records relating to:

- Candidates (e.g., teachers, teaching assistants)
- Clients (e.g., schools, educational institutions)
- Compliance (e.g., DBS checks, safeguarding documentation)
- Internal HR and company records
- Financial transactions

3. Reasons for Data Retention

CERT Solutions retains only that data that is necessary to effectively conduct its program activities, fulfil its mission and comply with applicable laws and regulations

4. 3. Retention Schedule

Record Type	Examples	Retention Period	Legal/Business Justification
Candidate Records	CVs, applications, interview notes, references	6 years from last contact	Limitation Act 1980; potential re-engagement
Placed Candidate Files	DBS checks, identity documents, right to work, contracts	6 years after placement ends	Safeguarding; audit and legal purposes
Client Records	School contracts, service agreements, communications	6 years after last engagement	Business recordkeeping; legal claims
Safeguarding & Compliance Docs	DBS certificates, training records, ID checks	6 years from date of last use	Legal safeguarding obligations
Financial Records	Invoices, payroll, tax records	6 years	HMRC requirements

Record Type	Examples	Retention Period	Legal/Business Justification
Marketing Data	Email marketing lists, consent forms	Until consent withdrawn or 2 years post last activity	GDPR - lawful basis for processing
Internal HR Records	Employee files, disciplinary records	6 years after employment ends	Employment law

5. Storage and Security

- All physical records are stored in locked cabinets with restricted access.
- Digital records are stored on secure, access-controlled systems.
- Cloud providers must meet industry-standard security protocols (e.g., ISO 27001).

6. Disposal of Records

- Digital data will be permanently deleted using secure deletion software.
- Paper records will be shredded or incinerated
- Deletion logs will be maintained for audit purposes.

7. Data Subject Rights

Under the **UK GDPR and Data Protection Act 2018**, individuals have the right to:

- Access their personal data
- Request correction or deletion
- Object to or restrict processing

Requests can be made by contacting the Data Protection Officer at: paul@cert-solutions.co.uk

8. Review and Updates

This policy is reviewed annually or in response to changes in legal or regulatory requirements.