

ELEVATE BEYOND LIMITED

Backup and Data Retention Policy

Supporting Every Step Forward

POLICY INFORMATION	
Version	2.0
Date Issued	September 2026
Next Review	September 2027 (and annually thereafter)
Policy Owner	Sulayman Cham — Founder and Director
ICO Registration	Data Controller, registration ZC149842
Company Number	17222138
Registered Address	Swan Building, 20 Swan Street, Manchester, M4 5JW
Website	www.elevate-beyond.co.uk

This document should be read alongside: GDPR and Data Protection Policy, Appropriate Policy Document, Safeguarding Policy. It sets out, in more operational detail than the GDPR policy, how Elevate Beyond's data is backed up, how long it is kept, and how it is destroyed.

Contents

1. About This Policy
2. Systems of Record
3. Backup
4. Retention Schedule
5. Deletion
6. Data Subject Rights and Breaches
7. Responsibilities

1. About This Policy

Elevate Beyond holds personal data about candidates, school contacts and its own business. Some of it is sensitive: DBS outcomes, references, safeguarding information, right to work documents. This policy sets out how that data is backed up, how long it is kept, and how it is destroyed. It applies to both partners and to any future staff, on every device and system used for company work.

Elevate Beyond is registered with the Information Commissioner's Office as a data controller, registration ZC149842.

DBS information is criminal offence data under Article 10 of the UK GDPR and section 10(5) of the Data Protection Act 2018. Processing it requires a condition in Schedule 1 of that Act and a separate Appropriate Policy Document, which Elevate Beyond holds and which should be read alongside this policy.

This policy is reviewed annually and updated immediately following any significant change to how the business stores or processes data.

2. Systems of Record

Company data lives in the following systems, and nowhere else:

- Google Workspace, including the shared drive — candidate files, school records, correspondence

- Xero — invoicing, timesheets, financial records
- DDC (Due Diligence Checking) — DBS applications, right to work and identity verification, and online/social media checks for candidates registered from 5 August 2026 onwards
- uCheck — DBS applications, right to work and identity verification for candidates registered before that date, who remain on uCheck
- APCS (Access Personal Checking Services) — QTS status and prohibition from teaching checks
- Sprintlaw e-signature platform — signed candidate and client agreements
- The Command Centre workbook / CRM — operational tracking of candidates, schools, placements and decisions
- The Single Central Record — the formal record of compliance checks

Working copies may sit temporarily on a partner's device while a task is in progress, but the cloud system is always the master record. No company data is stored only on a local device, a personal email account, a messaging app or removable media.

3. Backup

Cloud systems provide the primary backup. Google Workspace and Xero both retain version history and deleted-item recovery, and both partners' accounts have multi-factor authentication enabled. Devices used for company work are encrypted, password protected and set to lock automatically.

A quarterly export of the Command Centre workbook / CRM and the Single Central Record is taken and stored in a separate folder, so that an accidental overwrite can be recovered from a known good version.

Restore testing

Once a year, a restore is tested: a file is recovered from backup and checked. A backup that has never been restored is an assumption, not a backup.

4. Retention Schedule

Data is kept for as long as there is a lawful reason to keep it, and no longer. The schedule below governs all systems listed in section 2.

Where the Conduct of Employment Agencies and Employment Businesses Regulations 2003 require a longer minimum than any period below, the Conduct Regulations prevail. Regulation 29(2) requires records of every work-seeker and every hirer to be kept for at least one year from creation, and for at least one year after Elevate Beyond last provides services to that person or client.

Record	Retention Period	Reason
All work-seeker and hirer records where any action was taken on the application	Minimum 1 year from creation, and at least 1 year after we last provide services to that person or client	Conduct Regulations 2003, reg 29(2). "Action" is read broadly: a call, a screening note or a rejection email all count
Applications on which no action was taken	6 months, with the reason for applying the exemption recorded	Conduct Regulations 2003, reg 29(3)
Registered candidate, never placed	2 years from last contact, subject to the reg 29 minimum above	Sector norm; re-consent after that
Placed candidate: compliance file, references, agreements	6 years after the last assignment ends	Limitation Act 1980 period for contract claims

Record	Retention Period	Reason
DBS certificate content	No copy, scan or image of a certificate is retained after the recruitment decision. We retain only the certificate number, issue date, level, workforce type and the decision made	Certificate content is kept no longer than necessary, in line with gov.uk guidance on handling DBS certificate information. The number and date are retained longer because client schools require them for their Single Central Record
Right to work evidence	Duration of engagement plus 2 years	Statutory excuse against a civil penalty
Timesheets, invoices, financial records	6 years plus the current year	HMRC requirement
National Minimum Wage records	6 years	National Minimum Wage Regulations 2015, reg 59(8) as amended
Client school agreements	6 years after termination	Contract limitation
Safeguarding concerns or allegations about a candidate, and any DBS referral made	Long-term retention, having regard to KCSiE guidance on allegations. Period to be confirmed with Sprintlaw	Child protection; defence of historic claims
Marketing and outreach contacts	Until the contact objects or the relationship ends	Legitimate interests

Two points on the DBS row. First, agencies should not keep photocopies or scans of DBS certificates on file: record the detail, destroy the image. Second, there is no fixed statutory retention period for certificate content — the DBS Code of Practice sets none; the requirement is to keep it no longer than necessary once the recruitment decision is made.

5. Deletion

When a retention period expires, records are deleted from all systems including backups and trash folders, and the deletion is noted so the position can be evidenced. Paper is shredded. Devices are wiped before disposal or resale.

6. Data Subject Rights and Breaches

Access, correction and erasure

Candidates and school contacts may request access to their data, correction, or erasure where no other duty requires it to be kept. Requests go to Sulayman and are answered within one month. Where the Conduct Regulations or a safeguarding duty require retention, erasure is refused and the reason recorded.

Personal data breaches

A personal data breach — a lost device, an email sent to the wrong recipient, an unauthorised disclosure — is reported to Sulayman immediately and assessed the same day. Where the breach is likely to result in a risk to individuals, it is reported to the ICO within 72 hours of Elevate Beyond becoming aware of it. Affected individuals are told without undue delay where the risk to them is high. A record of every breach is kept, including those not reported.

7. Responsibilities

Sulayman Cham, Founder and Director, is the data controller contact and owns this policy. He is responsible for the annual restore test, for keeping the retention schedule under review, and for responding to data subject requests and breaches within the timescales above. Mohsin Habashi is

responsible for ensuring school and client data handled on the commercial side follows the same systems-of-record and retention rules.

Elevate Beyond Limited — Company No. 17222138 — info@elevate-beyond.co.uk — www.elevate-beyond.co.uk