Elevate-Ed Data Protection and Privacy Policy 2025–2026

Last Updated: September 2025
Next Review Due: September 2026
Reviewed by: Aaron Guy, Proprietor / DSL, Georgia Guy Director / QA

---

1. Introduction

Elevate-Ed is committed to protecting the personal data of children, families, staff, and commissioners. We collect and process information in line with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Keeping Children Safe in Education (2025)
- Working Together to Safeguard Children (2023)

This policy sets out how Elevate-Ed manages, stores, and shares data to ensure compliance and safeguard the welfare of learners.

It should be read alongside:

- Safeguarding Policy 2025–2026
- Online Safety Policy
- Staff Code of Conduct

---

2. Scope

This policy applies to:

- All learners engaged with Elevate-Ed
- Parents and carers where appropriate
- Schools, local authorities, and other commissioning parties
- Staff, freelance practitioners, volunteers, and QA roles

3. Principles of Data Processing

Elevate-Ed follows the seven principles of UK GDPR:

- **Lawfulness, fairness, transparency** – data collected and processed legally and clearly
- **Purpose limitation** – data used only for specific, legitimate purposes
- **Data minimisation** – only necessary data is collected
- **Accuracy** – data kept up to date
- **Storage limitation** – retained only as long as required
- **Integrity & confidentiality** – secure storage and handling
- **Accountability** – Elevate-Ed demonstrates compliance through records and procedures

4. Lawful Basis for Processing

Personal data is processed under Articles 6 & 9 of UK GDPR:

- **Legal obligation** – safeguarding, statutory reporting, employment law
- **Public task** – delivering education and associated services
- **Vital interests** – protecting children and young people in emergencies
- **Legitimate interests** – managing provision, QA, and communications
- **Consent** – for optional activities such as photographs/videos (consent always recorded in writing)

5. Data Protection Lead

The Proprietor (Aaron Guy) is the Data Protection Lead.
Where necessary, external advice will be sought from the Information Commissioner's Office (ICO) or legal services.

6. Types of Data Collected

- **Learner data** – personal details, EHCPs, referral forms, risk assessments, medical needs, emergency contacts, safeguarding records
- **Parental/carer data** – names, contact information, consent forms
- **Commissioner data** – contact details, referral agreements, SLAs
- **Staff/freelancer data** – personal details, DBS status, right-to-work documentation, self-declarations/disclosures, references, training records
- **Session data** – attendance, progress logs, reviews, safeguarding concerns

---

7. Safeguarding & Information Sharing

- Safeguarding records are securely retained until the learner's 25th birthday
- Records stored on a restricted Google Drive folder (2FA enabled; access limited to DSL & QA Lead)
- Records shared only with those who "need to know" (school DSL, LA officer, Virtual School)
- From August 2025, CADS referrals must be made by telephone; CADS provides written confirmation — reflected in Elevate-Ed practice
- Consent is sought for information sharing wherever possible, but safeguarding concerns may be shared without consent where a child is at risk of significant harm

---

8. Information Sharing with Commissioners

- Commissioners receive safeguarding and data assurance as part of the SLA
- Elevate-Ed does not commence delivery until due diligence checks are complete and the SLA is agreed in principle
- Information shared: safeguarding updates, progress reports, attendance summaries
- All sharing is documented in Elevate-Ed's secure records

---

9. Staff & Safer Recruitment Data

- Enhanced DBS checks (with barred list) required for all staff/volunteers in regulated activity

- Self-declarations/disclosures of criminal history collected at recruitment and annually
- Single Central Record (SCR) maintained securely
- Recruitment data includes identity verification, right-to-work checks, references, qualifications, safeguarding/Prevent training

---

10. Online Safety & Digital Data

- Learner use of devices strictly supervised at all times
- Filtering/monitoring applied on Elevate-Ed devices; learners' personal devices only used if agreed with parents/commissioners and under adult supervision
- Staff must not use personal devices to capture learner data unless DSL-approved; such data must be uploaded immediately and deleted from device
- Parents/visitors may not take photos/videos during sessions unless explicitly authorised by the DSL

---

11. Subject Access & Parental Requests

- Parents/carers commissioning directly (e.g., elective home education) may request access to their child's data
- Requests must be written; Elevate-Ed responds within one calendar month
- Safeguarding disclosures may be withheld if release would place a child at risk or compromise investigations

---

12. Retention of Data

- **Safeguarding records** – until learner's 25th birthday
- **Staff records** – duration of employment + 6 years
- **Recruitment data** – 6 months for unsuccessful applicants
- **Accident/incident reports** – minimum 3 years (longer if insurance requires)
- **Financial records** – 6 years~
- **Retention & Disposal** - If and when paper records are created they are then immediately digitised, originals are securely destroyed via cross-cut shredding or

confidential waste, unless legal/statutory duties require retention of the original.

---

13. Use of Personal Devices for Work Purposes

Staff may use personal mobile phones or personal devices for Elevate-Ed work purposes **only** under the following controlled conditions:

- **A dedicated work email/account must be used** (Elevate-Ed Google Workspace).
- The device must be **passcode-protected** and secured at all times.
- No learner information may be **stored permanently** on a personal device.
- Staff must **not** communicate with learners via personal phone numbers, personal email, or personal messaging apps under any circumstances.
- Staff may communicate with **parents/carers** using their work phone number (even if the device is personal), as long as communication remains professional and appropriate.

Evidence of Learning (Photographs & Video)

Staff may take photographs or video evidence of learning **on a personal device**, under *strict* conditions:

- **Parent/guardian consent must be in place.**
- Where staff are based in schools, **school consent/permissions** must also be respected.
- Any permitted recording must be:
    - **Uploaded immediately** to Elevate-Ed's secure system (Google Drive/Seesaw/Tapestry).
    - **Deleted from the device immediately after upload.**
- Personal devices must **never**:
    - Store learner photos/videos long-term
    - Back up learner images to personal cloud accounts (iCloud, Google Photos, OneDrive, WhatsApp, etc.)

- Sync with personal photos galleries automatically
- Be used for any non-work-related photography during sessions

- Failure to upload and delete promptly is treated as a **potential data breach** and must be reported to the DSL/Data Protection Lead **within 24 hours**.

Use of Apps & Communication Tools

Staff must only use **approved Elevate-Ed systems**, including:

- Elevate-Ed Google Workspace
- Secure cloud storage (Elevate-Ed-controlled only)

Staff must **not use**:

- SMS/text with learners
- WhatsApp, Messenger, Instagram, Snapchat
- Personal cloud storage (e.g., iCloud/Google Photos)
- Personal email accounts for any learner information

14. Data Breaches

- All suspected or actual breaches must be reported immediately to the DSL/Proprietor
- Serious breaches will be reported to the ICO within 72 hours, as required by law

---

15. Monitoring & Review

This policy will be reviewed annually or sooner if guidance changes.

Signed:
Aaron Guy - Proprietor / DSL
Georgia Guy - Director/QA
Date: September 2025