

ELEVATED

A Holistic Approach To The Education of Young People

Privacy Policy

- Date Adopted: 18th September 2025
- Review Date: September 2026
- Policy Lead: Alexandra Mcloughlin, Data Protection Lead

Approved by: Mark Aitken, Head of Provision

1. Statement of Intent

ElevatEd AP Ltd is committed to protecting the privacy and personal data of our students, parents/carers, staff, and partners. We comply fully with the UK General Data Protection Regulation (GDPR), the Data Protection Act 2018, and relevant safeguarding legislation. This policy explains how we collect, use, store, and protect personal data.

2. Guiding Principles

- Lawfulness, Fairness & Transparency: Data is processed fairly, lawfully, and openly.
- Purpose Limitation: Data is collected for specified, explicit, and legitimate purposes.
- Data Minimisation: Only relevant and necessary data is collected.

- Accuracy: Data is kept accurate and up to date.
- Storage Limitation: Data is retained only as long as necessary.
- Integrity & Confidentiality: Data is kept secure through technical and organisational measures.
- Accountability: ElevatEd AP Ltd demonstrates compliance with data protection obligations.

3. Scope and Definitions

- Scope: Applies to all personal data processed by ElevatEd AP Ltd relating to students, parents/carers, staff, contractors, and partners.
- Personal Data: Any information that identifies or could identify an individual.
- Special Category Data: Sensitive information such as health, ethnicity, or safeguarding records.
- Processing: Any action taken with personal data, including collection, storage, sharing, or deletion.

4. Roles and Responsibilities

- Data Protection Lead (DPL):
- Name: Alexandra Mcloughlin
- Contact: alex@elevate-ed.co.uk
- Responsibilities: Overseeing compliance, responding to data subject requests, reporting breaches.
- All Staff: Responsible for handling personal data securely and in line with training.
- Head of Provision: Ensures resources and systems are in place for compliance.

5. Data We Collect and Why

- Students: Contact details, academic records, attendance, safeguarding information, SEN/EHCP records, medical needs.
- Parents/Carers: Contact details, parental responsibility, emergency contacts.
- Staff: Employment history, qualifications, payroll, safeguarding and vetting checks.
- Other: Visitor records, CCTV (where applicable), contractor details.

Purpose of Data Collection:

- To deliver education and safeguarding responsibilities.
- To meet legal obligations (e.g., safeguarding, reporting to Local Authorities).
- To communicate effectively with parents/carers.
- To manage staff employment.
- To ensure health, safety, and wellbeing of students and staff.

6. Lawful Basis for Processing

ElevatEd AP Ltd processes data under the following bases:

- Legal Obligation: Safeguarding, employment law, and reporting duties.
- Public Task: Delivering education services in the public interest.
- Contract: Employment and service agreements.
- Consent: For optional activities (e.g., photos for marketing, additional services).
- Vital Interests: Protecting life or health in emergencies.

7. Data Sharing

We may share data with:

- Local authorities, social care, and safeguarding partners.
- The Department for Education (DfE) and Ofsted.
- External agencies for SEN support, counselling, or medical needs.
- Third-party service providers (IT systems, payroll, DBS checks).

We will never sell personal data.

8. Data Storage and Security

- Data stored securely on password-protected systems and locked storage.
- Access restricted to authorised staff only.
- Regular security audits and staff training undertaken.
- CCTV (if used) is retained for a limited period unless needed for investigations.

9. Data Retention

Personal data is retained only as long as necessary, in line with statutory guidance (e.g., pupil records retained until the child is 25 years old, safeguarding records retained in accordance with KCSIE and ICO guidance).

10. Rights of Data Subjects

Individuals have the right to:

- Access their personal data.
- Request correction of inaccurate data.
- Request erasure (where legally appropriate).
- Restrict or object to processing.
- Request data portability.
- Withdraw consent (where applicable).
- Complain to the Information Commissioner's Office (ICO).

11. Data Breach Procedures

- All staff must report suspected breaches immediately to the DPL.
- Serious breaches reported to the ICO within 72 hours.
- Affected individuals will be informed where there is a high risk to their rights and freedoms.

12. Training and Awareness

- All staff receive GDPR and data protection training on induction and refresher training annually.
- Specialist training provided for staff handling sensitive data.

13. Monitoring, Evaluation, and Review

- The DPL reviews data protection practices annually.
- This policy is reviewed every 12 months or sooner if legislation changes.

14. Related Policies

- Safeguarding Policy
- Staff Code of Conduct
- ICT and E-Safety Policy
- Whistleblowing Policy
- Recruitment & Selection Policy