ELEVATED

A Holistic Approach
To The Education of Young People

Data Protection and Information Management Policy

Date Adopted: 9th September 2025
Review Date: September 2026
Policy Lead: Data Protection Officer (DPO) – Alexandra Mcloughlin
Approved by: Mark Aitken, Head of Provision

1. Statement of Intent

ElevatEd AP Ltd is committed to protecting the personal data of all students, parents/carers, staff, volunteers, and partners. We handle data responsibly, lawfully, and transparently in line with the UK General Data Protection Regulation (GDPR), the Data Protection Act 2018, and relevant safeguarding requirements.

This policy explains how data is collected, stored, used, shared, and protected within ElevatEd, and outlines procedures for managing and responding to data breaches.

2. Guiding Principles

We follow the seven key principles of GDPR:

1. Lawfulness, fairness, and transparency – data is processed legally and openly.
2. Purpose limitation – data is collected for specific, legitimate purposes only.
3. Data minimisation – only data that is necessary is collected and processed.
4. Accuracy – data is kept up to date and accurate.
5. Storage limitation – data is kept only as long as necessary.
6. Integrity and confidentiality – data is kept secure.
7. Accountability – ElevatEd is responsible for demonstrating compliance.

3. Scope

This policy applies to:

- All personal data processed by ElevatEd (including digital and paper records).

All staff, volunteers, students, and parents/carers.

- All systems, software, and devices used to handle personal data.

4. Definitions

- Personal Data: Any information relating to an identified or identifiable individual (e.g., name, address, student ID).
- Special Category Data: Sensitive information (e.g., health, SEND, safeguarding).
- Processing: Any operation performed on data (collecting, storing, sharing).
- Data Subject: The individual to whom the data relates.
- Data Controller: ElevatEd, responsible for deciding how and why data is processed.
- Data Processor: Third parties processing data on behalf of ElevatEd.

5. Roles and Responsibilities

- Data Protection Officer (DPO):
- Ensures ElevatEd complies with data protection law.
- Provides advice, training, and monitoring.
- Acts as point of contact with the ICO (Information Commissioner's Office).
- Leadership Team:
- Ensure adequate resources for compliance.
- Monitor data handling practices.
- Staff and Volunteers:
- Handle data responsibly, following this policy.
- Report any breaches or concerns immediately.
- Students and Parents:
- Provide accurate information.
- Understand their rights under GDPR.

6. Rights of Data Subjects
Under GDPR, individuals have the right to:

- Be informed about how their data is used.
- Access their personal data (Subject Access Request).
- Rectify inaccurate or incomplete data.
- Erase data where there is no legal basis for its retention ("right to be forgotten").
- Restrict or object to processing under certain conditions.
- Data portability (transfer of data where applicable).

7. Data Collection, Storage, and Use

- Collection: Data collected is necessary for education, safeguarding, and operational purposes.
- Storage: Data stored securely on password-protected systems and locked filing cabinets.
- Use: Data used only for legitimate educational, pastoral, or administrative purposes.

- Retention: Data retained in line with statutory guidance (e.g., student records until 25 years

old).

8. Data Sharing

- Data will only be shared with:
- Local authorities, schools, and exam boards (where lawful and necessary).
- Social care, police, health services, and safeguarding partners (where required).
- Approved third-party service providers (with Data Processing Agreements in place).
- Data will never be sold to third parties.

9. Data Security

- Secure passwords and two-factor authentication used on systems.
- Regular staff training on safe data handling.
- Encryption of sensitive data when transferring.
- Secure disposal of old records (shredding, digital wiping).

10. Data Breaches
A data breach is any incident where personal data is:

- Lost, stolen, destroyed, accessed without permission, or shared inappropriately.

All breaches must be reported immediately to the DPO.

Flowchart: Data Breach Response
Step 1: Breach Identified
⬇️
Staff/volunteer detects data loss, theft, or misuse.
⬇️
Step 2: Report Immediately
⬇️
Notify the DPO within 24 hours.
⬇️
Step 3: Contain the Breach
⬇️
DPO/IT team take urgent steps (e.g., disable accounts, recover data, secure systems).
⬇️
Step 4: Assess Risk
⬇️
DPO evaluates severity and potential harm to individuals.

⬇️
Step 5: Notify ICO (if required)
⬇️
ICO informed within 72 hours if breach poses risk to individuals.
⬇️
Step 6: Notify Data Subjects (if required)
⬇️
Affected individuals informed if there is a high risk to their rights/freedoms.
⬇️
Step 7: Record & Review
⬇️
Incident recorded in Data Breach Log.
Preventative measures put in place to reduce future risk.

11. Monitoring and Review

- The DPO will conduct annual audits of data handling.
- All breaches and near misses will be reviewed to identify patterns.
- This policy will be reviewed annually or earlier if legislation changes.

12. Related Policies

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Staff Code of Conduct
- E Safety Policy
- Whistleblowing Policy