LEGACY EDUCATION
Data Protection & Privacy Policy

"Character Above All Else"

Approved by: Director
Responsible Person: Data Protection Lead / DSL
Last Review Date: December 2025
Next Review Due: December 2026

1. Statement of Intent

1.1. Legacy Alternative Provision (Legacy AP) is committed to protecting the privacy and rights of all individuals whose data we hold.

1.2. We collect and process personal information about students, parents, staff, and partner organisations in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

1.3. We recognise that much of our work involves sensitive personal information, and that confidentiality and trust are central to safeguarding and effective practice.

2. Purpose and Scope

2.1. This policy outlines how Legacy AP:

- Collects, stores, and uses personal data
- Ensures data is used fairly, lawfully, and transparently
- Protects data from loss, misuse, or unauthorised access
- Responds to data breaches and information requests

2.2. It applies to all staff, students, parents/carers, and partner agencies working with or on behalf of Legacy AP.

3. Roles and Responsibilities

3.1. Director (Data Controller):

- Responsible for ensuring Legacy AP complies with all relevant data protection laws and that appropriate systems are in place.

3.2. Data Protection Lead (DSL):

- Manages day-to-day compliance and data handling.
- Monitors data sharing and access control.
- Reports breaches and ensures staff training.

3.3. All Staff:

- Handle personal data securely and responsibly.
- Follow this policy and report any breaches immediately.
- Use Legacy AP systems and devices appropriately.
- Sign the **Acceptance of Data Protection Form** at the start of each Academic year

4. Lawful Basis for Processing

4.1. Legacy AP processes personal data under the following lawful bases (as defined by UK GDPR):

- Public task – fulfilling our educational and safeguarding responsibilities.
- Legal obligation – complying with statutory duties (e.g., safeguarding, attendance).
- Contract – managing staff and service agreements.
- Consent – where individuals have given clear permission (e.g., photography, marketing).
- Vital interests – to protect someone's life or wellbeing.

5. Types of Data Collected

5.1. Legacy AP may collect the following categories of information:

- Students:
  - Name, date of birth, contact details
  - Educational history and assessment data
  - Attendance, behaviour, and safeguarding records
  - Health or medical information (where relevant)
- Parents/Carers:
  - Contact information and emergency details
  - Consent forms and communication records
- Staff:
  - Employment details, training records, and DBS checks
- Partners/Referring Agencies:
  - Contact and commissioning details, reports, and correspondence

6. Data Storage and Security

6.1. All electronic data is stored securely using password-protected systems and encrypted devices.

6.2. Paper records are kept in locked cabinets in restricted areas.

6.3. Personal data is only accessible to authorised staff.

6.4. Data is retained only for as long as necessary in line with the Data Retention Schedule.

6.5. When no longer needed, data is securely deleted or shredded.

7. Sharing Data

7.1. Legacy AP only shares personal information when it is:

- Necessary for safeguarding, education, or health purposes;
- Required by law;
- With consent from the individual or parent/carer.

7.2. Data may be shared securely with:

- Referring schools or local authorities
- Police, social care, or health professionals (where appropriate)
- Ofsted or regulatory bodies (if applicable)

7.3. All sharing is logged and reviewed regularly.

8. Data Breaches

8.1. A data breach is any incident where personal information is lost, accessed, or shared without authorisation.

8.2. If a breach occurs:

1. The staff member must report it immediately to the Data Protection Lead / DSL.
2. The incident will be assessed and, if significant, reported to the Information Commissioner's Office (ICO) within 72 hours.
3. Individuals affected will be informed where there is a high risk to their rights or freedoms.

9. Subject Access Requests (SARs)

9.1. Individuals have the right to:

- Access their personal data;
- Request correction or deletion of inaccurate information;
- Object to processing in certain circumstances.

9.2. Requests must be made in writing to the Data Protection Lead, who will respond within one calendar month.

10.Consent and Photography

10.1. Where consent is required (e.g., for student photographs or promotional use):

- Consent will be clearly requested and recorded.
- Individuals may withdraw consent at any time.
- No images will be used without appropriate permissions.

11.Staff Use of Personal Data

11.1. Staff must:

- Keep all student and partner data confidential.
- Avoid storing personal data on private devices or email accounts.
- Use only approved systems (e.g., secure drives, password-protected files).
- Report any data security concerns immediately.

12.Monitoring and Review

12.1. This policy is reviewed annually or after any significant data incident.

12.2. All staff receive training on data protection and confidentiality during induction and refresher sessions.

13.Related Policies

13.1. This policy should be read alongside:

- Safeguarding & Child Protection Policy
- Staff Code of Conduct
- Online Safety Policy
- Equality, Diversity & Inclusion Policy