DATA PROTECTION & DATA SECURITY POLICY (Non-school Alternative Provision)

Policy title	Data Protection & Data Security Policy (Non-school Alternative Provision)
Applies to	All pupils, parents/carers and staff
Policy owner	Directors
Approved on	January 2026
Next Review	January 2027

1. Policy Statement

Applewood Learning is committed to protecting the rights and privacy of students, parents, and our workforce. We follow a "Privacy by Design" approach, ensuring that data protection is integrated into all our educational and administrative processes.

2. Lawful Basis for Processing

We process data only when a valid legal basis exists, primarily:

- **Legal Obligation:** For safeguarding and educational reporting.
- **Contractual Necessity:** To manage agreements with parents, staff and self-employed teachers.
- **Legitimate Interests:** For the efficient running of Applewood Learning Ltd.
- **Consent:** For optional activities like marketing or social media photos.

3. Data Categories Processed

- Identifying data (name, DOB, address)
- Contact details
- Safeguarding and SEN data (special category)
- Behaviour and attendance records
- Workforce data (DBS, right to work, payroll)
- Financial data (fees, invoices where applicable)

We process special category and criminal offence data only where permitted under Article 9 UK GDPR and Schedule 1 of the Data Protection Act 2018, primarily for safeguarding, employment checks, and provision of education and support services.

4. Specific Exclusions (CCTV, AI & Biometrics)

To ensure transparency, Applewood Learning declares:

- **No AI Processing:** We do not use Artificial Intelligence (AI) or machine learning algorithms to process, analysis, or profile personal data. No student or staff data is permitted to be entered into third-party AI tools (e.g., LLMs or automated grading systems).
- **No CCTV:** We do not operate Closed-Circuit Television or any form of video surveillance.
- **No Biometrics:** We do not collect or process biometric data (such as fingerprints or facial recognition).

5. Safeguarding and Data Protection (KCSIE Compliance)

In line with Keeping Children Safe in Education (KCSIE), Applewood Learning recognises that:

- **Safeguarding Trumps Privacy:** Data protection is not a barrier to sharing information to safeguard a child. We will share information with the Multi-Agency Safeguarding Hub (MASH) or Police without consent if a child is at risk of significant harm.
- **Filtering and Monitoring:** We utilise appropriate filtering and monitoring systems on our digital networks. Filtering and monitoring are carried out under the lawful bases of Legal Obligation and Legitimate Interests to ensure safeguarding and student welfare.
- **Transfer of Safeguarding Files:** When a student moves to a new setting, their safeguarding file will be transferred securely and separately from their main academic file.

6. Roles and Responsibilities

- **Directors:** Ultimate legal responsibility for GDPR compliance and ensuring sufficient resources are allocated for data security.
- **Data Protection Lead (DPL):** Manages the ROPA, oversees ICO reporting, and acts as the primary contact for data rights. Applewood Learning maintains a Record of Processing Activities (ROPA) in accordance with Article 30 UK GDPR. Note: Applewood Learning Ltd is not legally required to appoint a statutory Data Protection Office under UK GDPR. We have appointed a Data Protection Lead (DPL) to fulfil governance and compliance responsibilities.
- **Designated Safeguarding Lead (DSL):** Responsible for the secure storage and transfer of safeguarding files and ensuring the Single Central Record (SCR) is accurate.

- **All Workforce (Staff & Self-Employed Teachers):** Must maintain confidentiality, report breaches immediately, and only access data required for their specific role. All staff receive the following training:
- Mandatory annual data protection training
- Induction training for new staff/contractors
- Refresher training following incidents

7. Data Sharing with Third Parties

- **Lawful Sharing:** We share data with HMRC, the DfE, or Safeguarding Partners only when legally required.
- **Processors:** We use secure cloud/payroll providers bound by a Data Processing Agreement (DPA).
- **No Commercial Sharing:** We never sell or share personal data with third parties for marketing purposes.
- **International Data Transfers:** We do not knowingly transfer personal data outside of the UK. Where third-party systems involve international data processing, appropriate safeguards such as UK GDPR adequacy regulations or Standard Contractual Clauses are in place.

8. Data Security (Technical & Organisational)

- **Technical:** Multi-Factor Authentication (MFA) is mandatory for all workforce accounts. Sensitive data is encrypted at rest and in transit where technically feasible.
- **Physical:** Paper records are kept in locked, fireproof cabinets.
- **DBS Data:** A record of the DBS reference number and outcome is retained in the Single Central Record (SCR). We do not retain copies of the certificates themselves for longer than 6 months.
- **Contractor Protocols:** Self-employed teachers must sign a Data Processing Agreement (DPA) and are prohibited from taking photos of students on personal devices.
- We carry out Data Protection Impact Assessments (DPIAs) where processing is likely to result in a high risk to individuals' rights and freedoms.

9. Photographs and Media

We recognise that photographs and videos are sensitive personal data. Our approach to consent is determined by the age and capacity of the student:

- **Students under 18:** We will never take, store, or display photographs or videos without explicit written consent from a parent or legal guardian.
- **Students aged 18–25 (Adults):** Consent must be sought directly from the student. For students who may lack the mental capacity to provide consent, we will consult with their legal advocates or appointed representatives in accordance with the Mental Capacity Act 2005.
- **The Transition at 18:** When a student turns 18, any previous parental consent will be reviewed, and we will seek fresh consent directly from the student to ensure their adult rights are respected.
- **Right to Withdraw:** Consent may be withdrawn at any time by the person who provided it (the parent for minors, or the adult student). Upon withdrawal, images will be removed from all Applewood Learning platforms and records immediately.

10. Data Breach Management & ICO Reporting

Applewood Learning takes its responsibility to manage security incidents seriously. In the event of a personal data breach, we follow a strict protocol in accordance with the UK GDPR and the Data (Use and Access) Act 2025.

10.1 Internal Reporting

- All staff and self-employed teachers must report any suspected or actual data breach (e.g., lost laptop, misdirected email, unauthorised access) to the Data Protection Lead immediately upon discovery.

10.2 Assessment of Risk

- The Data Protection Lead will investigate the breach to determine if it is "likely to result in a risk to the rights and freedoms of individuals."

10.3 Reporting to the ICO

- **72-Hour Window:** If the breach is deemed "risky," we must notify the Information Commissioner's Officer (ICO) without undue delay and, where feasible, within 72 hours of becoming aware of it.
- **Required Information:** Our report to the ICO will include the nature of the breach, the categories and approximate number of individuals affected, the likely consequences, and the measures taken to mitigate the impact.
- **Late Reporting:** If we report after 72 hours, we must provide a reasoned justification for the delay.

10.4 Notifying Data Subjects

- If a breach is likely to result in a high risk to an individual's rights (e.g., identity theft or financial loss), we will notify the affected individuals directly and without undue delay so they can take protective action.

10.5 Documentation

- We maintain an internal Data Breach Log regardless of whether the breach was reported to the ICO. This log records the facts, the effects, and the remedial action taken.

11. Retention Periods

- **Student Records:** Retained for 6 years after the student leaves.
- **Safeguarding Records:** Retained until the individual's 25th birthday.
- **Workforce Records (Staff & Contractors):** Retained for 6 years after the end of the contract/employment for tax and legal purposes.

12. Individual Rights

Individuals have the right to:

- Right to object
- Right to restrict processing
- Right to data portability (where applicable)
- Right to withdraw consent
- Right not to be subject to automated decision-making
- Right of access (Subject Access Requests)
- Right to rectification

We will respond to all Subject Access Requests within one calendar month.

13. Contact and Complaints

We encourage individuals to raise concerns with us first so we can resolve issues promptly and fairly.

For any data concerns, contact the Data Protection Lead at carol.brooks@applewoodlearning.co.uk. If unsatisfied, you have the right to lodge a complaint with the Information Commissioner's Officer (ICO) or call 0303 123 1113.

VERSION CONTROL

We will review our documentation regularly and we reserve the right to amend our policies and procedures at any time.