GDPR Policy (1 year reviews)

April 2026

The Paddock is a calm and nurturing alternative provision in Shropshire, offering personalised, research-informed support for young people who need a smaller, more flexible approach to learning. We specialise in helping academically capable students who currently find mainstream environments overwhelming, providing a peaceful space where they can re-engage, rebuild confidence, and thrive.

This policy supports The Paddock's aim of ensuring that every young person is able to overcome barriers to learning and achieve their full potential. Our vision is to equip pupils with the skills, confidence and strategies they need to access education, enjoy education and to be ready to return to the most appropriate setting for them.

The Aims of The Paddock

The Paddock is committed to ensuring that all personal data relating to pupils, parents/carers, staff, governors, visitors, and other individuals is collected, stored, and processed in full compliance with UK data protection law. This policy applies to all personal data, whether held electronically or on paper.

Legislation & Guidance

Our GDPR policy follows the requirements of the UK GDPR and the Data Protection Act 2018, and aligns with guidance from the Information Commissioner's Office (ICO) and the Department for Education's information-sharing advice for safeguarding practitioners. It also complies with the Education (Student Information) Regulations 2005.

Definitions

The policy defines key GDPR terms such as *personal data*, *special category data*, *processing*, *data controller*, *data processor*, and *personal data breach*, ensuring all staff understand their responsibilities.

The Data Controller

The Paddock processes personal data for a range of purposes and is therefore the data controller.

Roles & Responsibilities

- **Directors** hold overall responsibility for GDPR compliance.
- **The Data Protection Officer (DPO)** oversees implementation, monitors compliance, and acts as the first point of contact for individuals and the ICO.
- **The Principal** acts as the representative of the data controller on a daily basis.
- **All staff** must follow the policy, keep data secure, report concerns, and contact the DPO when unsure about lawful processing or when a breach occurs.

Data Protection Principles

The Paddock follows the six GDPR principles:

- Lawfulness, fairness, transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security) The policy explains how the school ensures compliance with each principle.

Collecting Personal Data

The policy outlines lawful bases for processing, including legal obligation, public task, consent, and vital interests. It also explains conditions for processing special category and criminal offence data. Staff must only collect data that is necessary, accurate, and up to date.

Sharing Personal Data

Data is only shared when necessary and lawful—for example with safeguarding partners, contractors, emergency services, or when legally required. The school ensures third-party processors meet GDPR standards. International transfers follow UK GDPR rules.

Rights of Individuals

The policy explains:

- Subject Access Requests (SARs)
- Rights to rectification, erasure, restriction, objection
- Rights relating to automated decision-making
- Rights to data portability It also explains how SARs are handled, including identity checks, timescales, and exemptions.

Parental Access to Educational Records

Parents/carers have the right to access their child's educational record within 15 school days. The school may charge for copies.

Photos & Videos

The school obtains written consent for using pupil images and explains how images may be used. Parents are asked not to share photos of other pupils online.

Data Protection by Design & Default

The Paddock integrates data protection into all systems and processes, including DPIAs, staff training, privacy notices, and secure processing practices.

Data Security & Storage

The policy sets out expectations for secure handling of paper and digital records, password protection, encryption, and secure off-site use.

Disposal of Records

Data no longer required is securely destroyed, either internally or via a compliant third-party provider.

Personal Data Breaches

The policy includes a detailed breach-response procedure, including investigation, containment, ICO reporting within 72 hours, and communication with affected individuals when required.

Training

All staff receive GDPR training at induction and through ongoing CPD.

Monitoring

The DPO monitors compliance and reviews the policy annually.

Linked Policies

The GDPR policy links to the Online Safety Policy, Acceptable Use of ICT, Safeguarding and Child Protection Policy, Code of Conduct, and Privacy Policy.

Policy	**GDPR Policy**
Date created	April 2026
Date reviewed	
Date of Next review	April 2027
Signed	
Luke Baker	L. Baker