Mulberry Schools Trust
Data Protection Policy

Approval Body:	**Finance Committee**
Approval Date:	**November 2025**
Implementation Date:	**November 2025**
Review Date:	**November 2026**
Policy Version:	**1**

Introduction

The Mulberry Schools Trust aims to ensure that all personal data collected about staff, pupils, parents and carers, governors, visitors, and other individuals is collected, stored, and processed in accordance with UK data protection law. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

Legislation and Guidance

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA 2018)
- Protection of Freedoms Act 2012 (specifically regarding the use of biometric data)
- Education (Pupil Information) (England) Regulations 2005 (regarding parental access to educational records)

It is based on guidance published by the Information Commissioner's Office (ICO) and guidance from the Department for Education (DfE) on Generative Artificial Intelligence in education.

Definitions

Term	Definition
Personal Data	Any information relating to an identified, or identifiable, living individual. This includes name, identification number, location data, or online identifier.
Special Categories of Personal Data	Personal data which is more sensitive and needs more protection, including information about an individual's: Racial/ethnic origin, religious/philosophical beliefs, health (physical or mental), and biometrics (used for identification).
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, retrieving, using, disseminating, erasing, or destroying.
Data Subject	The identified or identifiable individual whose personal data is held or processed.
Data Controller	A person or organisation that determines the purposes and the means of processing personal data (i.e., Mulberry Schools Trust).
Data Processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The Data Controller

The Mulberry Schools Trust is the Data Controller. The Trust is registered with the ICO and has paid its data protection fee, as legally required.

Roles and Responsibilities
This policy applies to all staff, governors, and external organisations working on behalf of the Trust.

- **Governing Board**

The Governing Board has overall responsibility for ensuring the Trust complies with all relevant data protection obligations.

- **Data Protection Officer (DPO)**

The DPO is responsible for overseeing the implementation of this policy, monitoring compliance, and is the first point of contact for individuals and the ICO.
Our DPO is:

Satswana Ltd
Email: info@satswana.com
Telephone: 01252 516898
Address: Pembroke House, St Christopher's Place, Farnborough, Hampshire, GU14 0NH

- **All Staff**

Staff are responsible for:

a) Collecting, storing, and processing personal data in accordance with this policy.
b) Informing the school of any changes to their personal data.
c) Immediately contacting the DPO with any questions, concerns, or suspected data breaches.

Data Protection Principles
The Trust complies with the UK GDPR principles, ensuring personal data is:

1. Processed lawfully, fairly, and transparently.
2. Collected for specified, explicit, and legitimate purposes.
3. Adequate, relevant, and limited to what is necessary.
4. Accurate and, where necessary, kept up to date.
5. Kept for no longer than is necessary for the purposes for which it is processed.
6. Processed in a way that ensures it is appropriately secure.

Collecting and Sharing Personal Data
Lawful Basis for Processing
The Trust will only process personal data where there is one of the six lawful bases to do so.
Our primary lawful basis for core educational and administrative activities is:

- Article 6(1)(e): Public Task: Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller (i.e., running the school).

For Special Category Data (e.g., health, ethnicity), we rely on:

- Article 9(2)(g): Substantial Public Interest: Processing is necessary for reasons of substantial public interest, authorised by law (Schedule 1 of the DPA 2018).

Transparency and Statutory Sharing
Whenever we collect data, we will provide individuals with a Privacy Notice (for pupils, staff, etc.) explaining how we use and process their information.
We routinely share pupil information with:

- The Local Authority (LA).
- The Department for Education (DfE) via statutory data collections, such as the School Census, which transfers data to the National Pupil Database (NPD).
- Schools that pupils attend after leaving us.
- NHS and other welfare agencies (where legally required or with consent).

When sharing data with suppliers or contractors (Data Processors), we will ensure a legally binding contract is in place that guarantees compliance with UK data protection law.

Biometric Recognition Systems (Pupil Data)

The Trust uses pupils' biometric data (digital measurements, not full fingerprints) as part of an automated recognition system for the purpose of purchasing items from the school canteen and for the library to loan books. We comply with the Protection of Freedoms Act 2012.

- The school will get written consent from at least one parent/carer before we first process a child's biometric data.
- Parents/carers and pupils have the right to refuse or withdraw consent at any time. The school will provide alternative means of accessing the relevant services (e.g., a physical card or ID).
- If a pupil (regardless of parental consent) refuses to participate, the school will not process that data.

Artificial Intelligence (AI)

The Trust recognises that Generative Artificial Intelligence (AI) tools, such as generative chatbots, pose risks to sensitive and personal data.

- Staff and pupils are prohibited from inputting any personal data (including names, addresses, images, or safeguarding information) into unauthorised, public-facing Generative AI tools or chatbots where a legally compliant data processing agreement is not in place.[5]
- If personal and/or sensitive data is entered into an unauthorised generative AI tool, Mulberry Schools Trust will treat this as a Personal Data Breach, and the procedure in Appendix 1 will be followed.

Subject Access Requests (SARs)

Individuals (staff, pupils, or parents on a child's behalf) have the right to make a Subject Access Request to gain access to the personal information the Trust holds about them.

- Requests can be submitted in any form but must be immediately forwarded to the DPO.
- The Trust will respond without undue delay and within one calendar month of receipt (or receipt of any necessary identification).
- The ability of a child to understand their rights will be judged on a case-by-case basis. Generally, pupils aged 12 and above are regarded as mature enough to decide whether a parent/carer can access their data, requiring the pupil's express permission.

Data Protection by Design and Default

The Trust will put measures in place to integrate data protection into all data processing activities. This includes:

- Conducting Data Protection Impact Assessments (DPIAs) for any new processing that is likely to be high-risk (e.g., introducing new CCTV, AI, or biometric systems). The DPO will advise on this process.
- Ensuring all contracts with Data Processors are legally compliant.
- Integrating data protection into internal documents and training.

Data Security and Disposal

- Paper-based records and portable electronic devices containing personal data are kept under lock and key when not in use. Passwords must be robust, and encryption software must be used to protect all portable devices.
- Personal data that is no longer needed will be disposed of securely, in accordance with the Trust's Record Retention Schedule. Paper records are shredded or incinerated, and electronic files are overwritten or securely deleted.

Training

All staff and governors are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance[7], or the Trust's processes make it necessary.

Monitoring Arrangements

The Data Protection Officer (DPO) is responsible for monitoring compliance with this policy and providing advice and support for its regular review.

This policy will be formally reviewed, adopted, and approved by the Governing Board (or delegated committee/senior leader) on an annual basis, or sooner if:

- There are changes to UK data protection legislation.
- The Trust introduces new, high-risk data processing activities (e.g., new technology or systems).
- The Trust is advised to do so by the Data Protection Officer or the Information Commissioner's Office (ICO).

The Governing Board is ultimately responsible for ensuring the policy is implemented and that the Trust remains accountable for its compliance.

Links with Other Policies

This data protection policy is linked to our:

- Privacy Notices (for Pupils, Staff, Governors)
- Freedom of Information Publication Scheme
- Safeguarding and Child Protection Policy
- CCTV Policy
- ICT and Online Safety Policy
- Record Retention Schedule

Appendix 1: Personal Data Breach Procedure
In the unlikely event of a suspected data breach, the following steps will be taken:

1. Immediate Discovery and Local Reporting

- *Any staff member who discovers or suspects a breach must immediately inform their Headteacher or line manager.*
- *The staff member must provide all known details, including what data is involved, where it is located, and how the breach occurred.*

2. Escalation to the Trust and DPO

- *The Headteacher must immediately escalate the incident to the designated Senior Trust Executive (e.g., the CEO, COPO, or Director of Operations) and the Data Protection Officer (DPO) - this ensures the legal entity (The Trust) is aware of the potential implications and liabilities immediately and can initiate central containment measures.*

3. Investigation and Triage

- *The DPO (or designated lead), in collaboration with the Senior Trust Executive, will formally lead the investigation to determine:*

a) The nature and scope of the breach.
b) *The risk to individuals' rights and freedoms.*

4. Containment & Recovery

- *Steps will be taken immediately to contain the breach (e.g., shutting down the affected system, recovering lost data, changing passwords). The Central Trust IT Team/Contractor will execute these actions under DPO guidance.*

5. Reporting to the ICO

- *If the breach results in a high risk to individuals, the DPO will report it to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of it.*

6. Notifying Data Subjects

- *If the breach is likely to result in a high risk to the rights and freedoms of individuals, the Trust will inform those affected without undue delay, following the DPO's advice.*

7. Record Keeping

- *All breaches, regardless of whether they are reported to the ICO, will be documented internally and shared with the Governing Board for their oversight and review of the Trust's risk register.*