



DATA PROTECTION POLICY

Table of contents

1.	Purpose
2.	Scope
3.	Legislative Context
4.	Policy Statement
5.	Governance and Roles
6.	Lawful Processing and Transparency
7.	Records, Mapping and Risk Management
8.	Data Security and Access Controls
9.	Data Sharing and Transfer
10.	Data Subject Rights
11.	Data Breaches and Incident Management
12.	Training and Awareness
13.	Monitoring and Review
14.	Related School Policies and Procedures

1. Purpose

The purpose of this policy is to ensure that personal and sensitive data is handled securely, lawfully and transparently, in line with UK data protection legislation and statutory guidance. The policy supports safeguarding, privacy, and trust across the school community and forms part of the school's wider approach to online safety and information security.

2. Scope

This policy applies to:

- All personal data processed by the school
- All staff, volunteers, governors and contractors
- Data subjects including staff, learners and parents/carers
- All digital and paper-based records
- All third party processing data on behalf of the school

3. Legislative Context

The school complies with all applicable data protection legislation, including:

- [UK General Data Protection Regulation \(GDPR\)](#)
- [Data Protection Act 2018](#)
- [Freedom of Information Act](#)
- [Relevant guidance from the Information Commissioner's Office \(ICO\)](#)

4. Policy Statement

The school recognises its role as a Data Controller and is committed to ensuring that personal data is:

- Processed lawfully, fairly and transparently
- Collected for specified and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and kept up to date
- Retained only for as long as necessary
- Secured against unauthorised access, loss or misuse#

Data security is recognised as a safeguarding responsibility and is embedded across leadership, governance and daily practice.

5. Governance and Roles

❖ Data Protection Officer (DPO)

The school will appoint a Data Protection Officer (internal or external) who:

- Provides independent advice and monitoring of compliance
- Supports Data Protection Impact Assessments (DPIAs)
- Acts as the point of contact with the ICO
- Reports directly to senior leadership and governors

The DPO operates independently and is supported with appropriate time, access and resources.

❖ Governors

Governors:

- Approve and review data protection policies
- Provide strategic oversight of compliance and risk
- Ensure adequate resources are allocated
- Receive reports on data breaches, audits and risks

❖ Senior Leaders and Staff

Senior leaders ensure that:

- Data protection is embedded into systems and culture
- Staff receive appropriate training

- Procedures are implemented consistently
- Data breaches are managed in line with school policy and in accordance with ICO guidance

All staff and governors are responsible for handling personal data securely and reporting concerns or incidents promptly.

6. Lawful Processing and Transparency

The school will:

- Identify and document lawful bases for processing personal data
- Apply additional conditions for processing special category data
- Maintain clear and accessible Privacy Notices for learners, parents/carers, staff and governors
- Ensure data subjects understand their rights
- Ensure consent is considered and established with data subjects and used only where appropriate and never as a default where a public task or legal obligation applies.

7. Records, Mapping and Risk Management

The school will maintain:

- A Record of Processing Activities (RoPA)
- A data asset register, including third-party and cloud services
- Clear retention and disposal schedules
- Data Protection Impact Assessments (DPIAs) for new or high-risk processing

Data protection is considered at the design stage of any new system or process ("data protection by design and default").

8. Data Security and Access Controls

The school will ensure that:

- Access to personal data is role-based and restricted
- User accounts are protected by strong authentication
- Devices accessing personal data are secured and encrypted where appropriate
- Personal data is stored only on approved systems
- Cloud services meet UK data protection and security requirements
- Third-party contracts include appropriate data processing clauses
- Paper records are stored securely and disposed of appropriately.

9. Data Sharing and Transfer

Personal data will only be shared:

- Where there is a lawful basis
- With appropriate safeguards in place
- Using secure transfer methods
- With approved third parties

Additional care is taken when data is accessed remotely or transferred off-site.

10.Data Subject Rights

The school will uphold all data subject rights, including:

- Right to be informed
- Right of access (Subject Access Requests)
- Right to rectification
- Right to erasure (where applicable)
- Right to restrict or object to processing

Procedures are in place to manage requests within statutory timescales.

11.Data Breaches and Incident Management

The school will:

- Maintain clear procedures for reporting and managing data breaches
- Assess the risk to individuals' rights and freedoms
- Notify the ICO within 72 hours where required
- Record all breaches and near-misses
- Use learning from incidents to improve practice

Data breaches are treated as serious incidents and may also trigger safeguarding procedures where appropriate.

12.Training and Awareness

The school will ensure that:

- All staff and governors receive regular data protection training
- New staff receive training as part of induction
- Targeted training is provided where roles require it
- Learners are taught about privacy and data protection as part of the curriculum, in an age-appropriate way

13.Monitoring and Review

This policy will be:

- Reviewed at least annually
- Updated in response to changes in legislation, guidance or risk
- Supported by audits and compliance checks

14.Related School Policies and Procedures

This Data Security Policy should be read alongside the school's:

- **Safeguarding Policy**

- **Online Safety Policy**
- **Technical Security Policy**
- **Cyber Security Policy**

Version control table

Version	Date	Changes	Approval
1	2026	Policy re-written to align with Online Safety and related policies.	SO