Data Protection Policy

This policy applies to Steephill School, including the EYFS setting.

Policy Author: Helen Millward Headteacher

Updated: September 2025

Date for Review: September 2026

Policy statement

Steephill School recognises the importance of data protection and privacy in maintaining trust, safeguarding pupils and staff, and complying with legal obligations.

This policy:

- Complies with the Data Protection Act 2018 and GDPR.
- Aligns with KCSIE 2025 safeguarding requirements.
- Applies to all personal data of pupils, staff, governors, parents, and visitors.

This policy covers all personal data:

- Electronic and paper records
- Emails, cloud storage, and databases
- CCTV and other surveillance recordings
- Data relating to pupils, staff, parents, governors, contractors and visitors

Roles & Responsibilities

Data Protection Officer (DPO)

- Provides guidance on compliance and good practice
- Monitors data processing and audits records
- Reports to governors termly on data protection matters

Headteacher

- Overall responsibility for school compliance
- Ensures adequate staff training and policy enforcement

Governors

- Approve policy and monitor compliance
- Review data protection reports termly

Staff

- Handle personal data responsibly and securely
- Report breaches immediately to the DPO
- Complete annual data protection training

Pupils and parents

- Pupils educated on data rights appropriate to their age
- Parents informed of how their data is used

Lawful basis for processing

Steephill School processes personal data under the following lawful bases:

- **Consent**: where explicit permission is required
- **Contractual necessity**: e.g., employment or enrolment agreements
- **Legal obligation**: statutory duties for safeguarding, health, or reporting
- **Vital interests**: safeguarding pupils' well-being
- **Public task**: delivering education and school services
- **Legitimate interests**: with minimal intrusion and robust safeguards

Data Subject Rights

Individuals have the right to:

- Access their personal data (Subject Access Requests)
- Request correction of inaccurate data
- Request erasure where lawful
- Restrict or object to processing
- Withdraw consent where applicable
- Lodge complaints with the Information Commissioner's Office (ICO)

All requests should be directed to the DPO. A response is issued within one month.

Data collection and storage

- Collect only data necessary for school purposes

- Secure storage using:
    - **Encrypted systems** (e.g., Engage, CPOMS, Atom Learning)
    - **Locked physical storage** for paper records
- Access restricted to authorised personnel only

Data sharing and third parties

- Only share data when lawful and necessary
- Written agreements in place with third-party processors
- Parents informed when their child's data is shared externally
- Examples of sharing:
    - Local authorities for statutory reporting
    - Health and safeguarding services
    - Educational technology platforms (GDPR-compliant)

Data retention and deletion

Retention schedules based on statutory guidance:

Data Type	Retention Period
Pupil records	Until age 25
Staff records	6 years post-employment
Financial records	7 years

Secure deletion when data is no longer required.

Security measures

- Strong passwords and multi-factor authentication
- Role-based access control for systems
- Encryption of sensitive electronic data
- Physical security of paper records
- Regular audits and monitoring of access logs

Breach Management

- All breaches reported immediately to the DPO
- DPO investigates and logs the incident
- High-risk breaches reported to the ICO within 72 hours
- Parents notified where pupil data is affected
- Review and remedial action taken to prevent recurrence

Breach Flowchart:

1. Incident identified → staff reports to DPO
2. Initial assessment → risk evaluation and logging
3. Containment & mitigation → limit exposure
4. Notification → ICO & affected individuals if required
5. Review & lessons learned → update policy/procedures

Training and awareness

Annual staff training on GDPR and school procedures

Induction training for new staff

Pupil awareness sessions appropriate to age and curriculum

Parental guidance provided via newsletters and school website

Policy Review

- Reviewed annually or sooner if legislation changes
- Reviewed by Headteacher, DPO, and governors
- Staff and governors must acknowledge understanding of updates