



THE MOUNTBATTEN SCHOOL

Data Retention Policy

September 2026

Review Date: September 2027

Whitenap Lane Romsey Hampshire SO51 5SY
t: 01794 502502 e: info@mountbatten.school
w: www.mountbatten.school Company No. 07560175

1. Data Retention Policy

This policy outlines the guidelines and procedures for managing the retention and disposal of personal data in compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and relevant education sector guidance.

The aim is to ensure that personal data is retained only for as long as necessary for legal, administrative, and educational purposes, and is disposed of securely to protect individuals' privacy. This policy also covers data stored in email, cloud systems, learning platforms, backups and removable media.

1.1 Scope

This policy applies to all staff, trustees, contractors, and visitors, and to all personal data held in any format, including staff, pupil, parent, trustee, and supplier records. It also covers photographs, videos, CCTV, biometric data (e.g. cashless catering fingerprints), health/medical records, electronic messaging services used for school business, and information held within cloud-based systems and collaboration platforms, including Microsoft 365 services (such as Exchange Online, Teams, SharePoint and OneDrive), educational applications, and other approved third-party systems.

1.2 Legal Framework

This policy meets the requirements of:

- UK GDPR and Data Protection Act 2018
- Freedom of Information Act 2000
- Education Act 1996 and related legislation
- Limitation Act 1980
- Department for Education statutory guidance
- Protection of Freedoms Act 2012 (where biometric data is processed)
- IRMS (Information and Records Management Society) Schools Toolkit

1.3 Retention Principles

1. Personal data will be kept only for the minimum period necessary.
2. Retention periods will be based on statutory requirements, DfE guidance, or operational needs.
3. Data will be regularly reviewed, and items no longer required will be securely destroyed.
4. Anonymised data may be retained longer for statistical purposes.
5. A formal annual review of all data sets and backups will be carried out by the Data Protection Officer (DPO) and documented in an audit log.
6. Retention periods and disposal requirements will be reflected within the school's Record of Processing Activities (ROPA) and reviewed annually to ensure ongoing compliance with data protection legislation and operational requirements.

Personal data will be retained in accordance with the UK GDPR principles of lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability.

1.4 Secure Disposal

When the retention period expires, records will be securely disposed of:

- Paper records: cross-cut shredded or incinerated.
- Electronic records: securely deleted so they cannot be recovered.
- Third-party processors: required to follow equivalent secure disposal processes.
- Personal data retained within cloud and offsite backups will be subject to the organisation's backup retention cycle and will be securely deleted when backup media reaches the end of its lifecycle.

- Electronic media will be securely erased using industry-recognised methods or physically destroyed where appropriate.

1.5 Data Subject Rights and Retention

The school will comply with individuals' rights under UK GDPR, including the right to erasure where applicable. Requests for deletion of personal data will be considered on a case-by-case basis. Where the school is required to retain records for legal, regulatory, safeguarding, operational, or public interest reasons, the information may be retained for the relevant retention period notwithstanding such a request.

1.6 Roles and Responsibilities

- Governing Body: ensures the school has a compliant policy.
- Headteacher: overall accountability for data management.
- Data Protection Officer (DPO): provides independent advice, monitors compliance, supports audits, and acts as a point of contact with the Information Commissioner's Office (ICO).
- All Staff: responsible for following retention rules and reporting breaches.

1.7 Monitoring and Review

This policy will be reviewed annually or earlier if:

- New legislation or guidance is issued.
- A significant data breach occurs.
- An internal audit recommends changes.

1.8 Related Policies

- Data Protection Policy
- Freedom of Information Policy
- Safeguarding and Child Protection Policy
- IT Acceptable Use Policy

2. Data Retention Schedule

Category	Record Type	Retention Period	Legal Basis / Guidance	Disposal Method
Pupil Records	Admission registers	Date of last entry + 6 years	Pupil Registration Regulations 2006	Shred / Secure wipe
Pupil Records	Pupil record (core file)	DOB + 25 years	Limitation Act 1980, safeguarding	Shred / Secure wipe
Pupil Records	Special Educational Needs (SEN) files	DOB + 25 years	Limitation Act 1980, SEND Code of Practice	Shred / Secure wipe
Pupil Records	Attendance registers	3 years	Pupil Registration Regulations 2006	Shred / Secure wipe
Safeguarding	Child Protection files	DOB + 25 years	Keeping Children Safe in Education	Shred / Secure wipe

Safeguarding	Allegation investigations (staff)	Termination + 10 years	DfE guidance	Shred / Secure wipe
Curriculum	Curriculum planning	Current year + 3 years	Operational need	Shred / Secure wipe
Curriculum	Exam papers (external)	6 months	Exam board regulations	Shred / Secure wipe
Personnel / HR	Staff personnel file	Termination + 6 years	Employment law	Shred / Secure wipe
Personnel / HR	Recruitment records (unsuccessful applicants)	6 months	Equality Act 2010	Shred / Secure wipe
Payroll / Finance	Payroll records	Current tax year + 6 years	HMRC requirements	Shred / Secure wipe
Governance	Governing Body minutes	Permanent	Corporate governance	Archive securely
Health & Safety	Accident reporting – pupils	DOB + 25 years	Limitation Act 1980	Shred / Secure wipe
Health & Safety	CCTV footage	31 days	ICO guidance	Automatic deletion / secure overwrite
Administrative	Visitors' books	6 years	Health & Safety	Shred / Secure wipe
Communications	Email Correspondence	2 years. Emails forming part of a pupil, staff, contract, safeguarding or complaint record should be retained in accordance with the relevant retention category.	Operational need	Shred / Secure wipe
Health/Medical	Care plans, medication logs	DOB + 25 years	Operational need	Shred / Secure wipe
Photographs and Video		Until consent withdrawn or 1 year after pupil leaves unless required for archives.	Operational need	Shred / Secure wipe
HR/Staff	Training and CPD Record	Termination + 6 years	Operational need	Shred / Secure wipe
HR/Staff/Student	Pupil/Staff Investigation	Resolution + 6 years	Operational need	Shred / Secure wipe
Procurement and Contracts	Supplier Contracts	Contract end + 6 years	Operational need	Shred / Secure wipe

Procurement and Contracts	Data Processing Agreements	Contract end + 6 years	Operational need	Shred / Secure wipe
Pupil Records	Safeguarding Records	DOB + 25 years	Keeping Children Safe in Education	Shred / Secure wipe
Pupil Records	Child Sexual Abuse	DOB + 75 years	Keeping Children Safe in Education	Shred / Secure wipe
Communications	Routine call recordings	6 months	UK GDPR (Public Task / Legitimate Interests), operational need	Secure Deletion
Complaints	Formal Complaints	Resolution + 6 years	Limitation Act 1980, operational need	Shred / Secure wipe
SEND	EHCP Correspondence	DOB +25 years	SEND Code of Practice, Limitation Act 1980	Shred / Secure wipe
Exclusions	Permanent Exclusion Record	DOB + 25 years	DfE guidance, Limitation Act 1980	Shred / Secure wipe
Governance	Trustee Declarations of Interest	Term end + 6 years	Charity Commission guidance, governance requirements	Shred / Secure wipe
IT	Security Logs	12 months	UK GDPR, Cyber Security and operational need	Secure deletion
Data Protection	Data Breach Record	6 years	UK GDPR accountability principle	Shred / Secure wipe
Data Protection	Subject Access Request Records	3 years after closure	UK GDPR, ICO guidance	Shred / Secure wipe

Retention periods may be extended where safeguarding concerns, statutory inquiries, legal claims or regulatory investigations require longer retention.

3. Sample Secure Destruction Log

This log must be completed whenever personal data is securely destroyed.

Date of Destruction	Record Description	Category	Method of Destruction	Authorized By
---------------------	--------------------	----------	-----------------------	---------------

The DPO will keep destruction logs and breach/audit records for at least 6 years.

All contracts with processors must include explicit clauses on retention, secure deletion, and provision of destruction certificates upon request.

Policy approved by the Human Resources Committee Date

Signed
Chair of Human Resources Committee

Date.....