

THE MOUNT SCHOOL

DATA PROTECTION, PRIVACY AND RECORDS MANAGEMENT POLICY

2026-2027

Policy detail	Information
Version	2.2
Policy writer	Euan Burton-Smith
Data Protection Lead	Chris Sellers
Last updated	September 2026
Effective from	1 September 2026
Review date	August 2027
Approval	Approved by Chris Sellers - Director / Proprietor

This policy should be read with the Safeguarding and Child Protection Policy, Staff Code of Conduct, Acceptable Use of Technology Policy, Online Safety Policy, CCTV arrangements, Safer Recruitment Policy, Complaints Policy, Records Retention Schedule and relevant privacy notices.

1. Purpose and scope

Data protection is an important legal, professional and safeguarding responsibility. The Mount School collects, creates, stores, uses and shares personal data about pupils, parents/carers, staff, applicants, volunteers, contractors, visitors and other individuals in the course of providing education, care and employment.

The School is a controller where it determines the purposes and means of processing. This policy applies to paper and electronic records, photographs, video and audio, CCTV, emails and messages, cloud systems, the MIS, filtering and monitoring information, artificial intelligence tools, portable devices and records created or accessed away from the School.

Employees, volunteers and contractors acting on behalf of the School must comply with this policy and any role-specific instructions. A contractor is not automatically a separate controller merely because they are a contractor: their legal status depends on what they actually determine about the purposes and means of processing.

2. Legal and regulatory framework

The principal framework is the UK GDPR and Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025 (DUAA), together with applicable Privacy and Electronic Communications Regulations requirements. The DUAA amends and builds on the existing UK data-protection regime; it does not replace UK GDPR or the Data Protection Act 2018.

The School also has regard to current Information Commissioner's Office guidance, DfE data-protection guidance as a sector benchmark, KCSIE 2026, the current EYFS framework, safeguarding duties, employment law, the Independent School Standards and relevant contractual and records-management obligations.

3. Key definitions

Term	Meaning
Controller	Determines the purposes and means of processing and is accountable for compliance.
Processor	Processes personal data on behalf of a controller under instructions and an appropriate contract.
Personal data	Information relating to an identified or identifiable living person.
Processing	Any operation on personal data, including collecting, creating, storing, accessing, using, sharing, altering, retrieving, archiving and deleting.
Special category data	Data revealing racial/ethnic origin, political opinions, religious/philosophical beliefs, trade union membership, genetic/biometric identification data, health, sex life or sexual orientation.
Criminal offence data	Data about criminal convictions, offences or related security measures. It is NOT special category data, but has its own additional legal protections.
Personal data breach	A security breach leading to accidental/unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data.
DPIA	Data Protection Impact Assessment: a structured assessment used before high-risk processing.

4. Data protection principles

- lawfulness, fairness and transparency;
- purpose limitation;
- data minimisation;
- accuracy;
- storage limitation;
- integrity and confidentiality (security); and
- accountability - the School must be able to demonstrate compliance.

Privacy by design and default must be considered when new systems, apps, EdTech products, AI tools, CCTV/monitoring arrangements or data-sharing activities are introduced.

5. Governance and responsibilities

Chris Sellers is designated as the School's Data Protection Lead. The 2025-2026 policy described him as the Data Protection Officer. This has been changed because a person formally appointed as a DPO under UK GDPR must satisfy statutory independence, expertise, resourcing and conflict-of-interest requirements. The School will record whether a statutory DPO is legally required and, if one is formally appointed, will ensure those requirements are met.

Role	Responsibilities
Director / Proprietor	Strategic oversight, resources, risk and assurance; ensures compliance arrangements are in place.
Data Protection Lead	Coordinates privacy notices, rights requests, breaches, complaints, DPIAs, contracts, training, records management and ICO liaison.
Headteacher	Operational implementation; ensures safeguarding and data protection operate together and that staff escalate concerns promptly.
SLT / managers	Ensure processing in their areas is lawful, necessary, secure, documented and reviewed.
All staff / authorised users	Use approved systems; protect information; recognise and report breaches, SARs and complaints; complete training.
Processors / suppliers	Act under compliant contracts/instructions and provide appropriate security, confidentiality and breach support.

6. Lawful bases for processing

The School must identify a lawful basis for each processing purpose. Depending on the context, this may include contract, legal obligation, legitimate interests, public task where the underlying task/function has a clear basis in law, vital interests, consent or another lawful basis available under UK GDPR.

Consent will not be used simply because it appears convenient. Where relied on, it must be freely given where required, specific, informed, unambiguous and capable of withdrawal.

For ordinary legitimate interests, the School will consider purpose, necessity and balancing against the individual's rights and freedoms. The DUAA also introduced recognised legitimate interests for specified purposes. These will only be relied on where the statutory condition genuinely applies.

Special category data requires an additional Article 9 condition. Criminal offence data requires Article 10/DPA 2018 authority and safeguards. The School will maintain an appropriate policy document where legally required.

7. Safeguarding and information sharing

Data protection law does not prevent necessary safeguarding information sharing. The welfare and protection of the child is a primary consideration. Staff must share relevant information with the DSL/DDSL and appropriate agencies where there is a lawful and necessary basis.

Consent is not required where seeking it would place a child at risk, prejudice the prevention or detection of crime, or otherwise be inappropriate. Staff must never promise absolute confidentiality to a child or adult where safeguarding information may need to be shared.

Safeguarding records must be accurate, factual, chronologically clear, secure and access-controlled. Safeguarding information must not be disclosed wholesale in response to a rights request without considering exemptions, third-party information, child welfare and other legal restrictions.

8. Professional record keeping

Personal data and records created by staff must be accurate, relevant, proportionate and professional. Opinions should be identified as opinions and attributed where appropriate.

The possibility that an individual may later obtain access must not deter staff from recording necessary safeguarding, disciplinary, pastoral, medical, SEND or educational information. Records should be written on the basis that the author could professionally justify their accuracy, relevance and tone.

Factual inaccuracies should be corrected through the approved system while preserving an audit trail where required.

9. Data minimisation, access and permissions

Staff may only access information necessary for their role. Technical ability to open a record does not create a right to view it. Curiosity access is prohibited.

Access privileges will be reviewed, role-based where practicable, and removed promptly when staff leave or change role. Shared accounts should be avoided unless technically necessary and appropriately controlled.

10. Data security - digital and paper

- use School approved accounts, systems and storage;
- use strong unique passwords and multi-factor authentication where provided or required;
- lock screens when devices are unattended;
- do not use personal email accounts for School personal data;
- check recipients, attachments and permissions before sending or sharing information;

- use BCC or approved bulk-mail tools where recipients should not see one another's addresses;
- keep paper records secure and out of public view;
- use authorised, encrypted removable media only where necessary;
- report phishing, malware, lost devices, misdirected emails and suspected account compromise immediately;
- dispose of confidential paper and electronic records securely.

The blanket rule in the old policy prohibiting any personal data from leaving the premises is replaced by a controlled approach. Secure authorised remote access and off-site processing may be used where necessary and protected by appropriate technical and organisational measures.

11. Personal devices and remote working

Personal devices must not be used to store School personal data unless expressly authorised under a defined and secured arrangement. School data should remain in approved systems wherever practicable.

Remote working must protect screens, conversations and paper records from unauthorised access. Sensitive documents should not be printed or retained at home unless specifically authorised and securely managed.

12. Emails, messaging and communications

School-approved communication channels must be used for pupil, parent and staff business. Disappearing-message services or personal social-media accounts must not be used for School records that require retention.

Where material safeguarding or management information is received through an informal channel, it must be transferred promptly to the appropriate School record.

13. Photographs, video, audio and CCTV

Images and recordings may be personal data and, in some circumstances, sensitive safeguarding evidence. The School will identify a lawful basis, provide appropriate transparency, restrict access and apply defined retention.

Safeguarding or evidential recordings must not be deleted simply because publicity consent is absent. Conversely, holding an image for safeguarding or administration does not automatically authorise its use for marketing or publicity.

CCTV will be operated for defined purposes with appropriate signage, privacy information, access controls, disclosure procedures and retention. A separate CCTV Policy may provide the detailed operational arrangements.

14. Filtering and monitoring information

Online filtering and monitoring can generate sensitive information about pupils and staff. Access to alerts and monitoring data must be limited to authorised, trained staff and handled in accordance with safeguarding and data-protection procedures.

New or materially changed monitoring arrangements will be assessed for privacy risk and may require a DPIA. Privacy information should explain the purpose, broad scope, access and retention of relevant monitoring data.

15. Generative AI and automated processing

Staff must not enter identifiable pupil, parent, staff, safeguarding, SEND, medical, HR or other confidential information into public or unapproved generative-AI tools.

Before introducing an AI-enabled service processing personal data, the School will assess controller/processor roles, lawful basis, transparency, security, retention, training use, international transfers, human oversight and whether a DPIA is required.

AI output must be checked by a competent human and must not replace professional safeguarding judgement.

The DUAA expands the circumstances in which significant solely automated decisions may be made, but safeguards still apply. The School will not rely on the new recognised legitimate interests basis for significant solely automated decision-making, because that basis is excluded for this purpose; special-category data remains subject to additional restrictions.

16. EdTech, processors and procurement

Before procuring a processor, EdTech platform or cloud service, the School will consider the nature and volume of data, purpose, security, data location, retention/deletion, subprocessors, international transfers, support access and breach handling.

Processor contracts must contain the terms required by data-protection law. Suppliers must not repurpose School personal data for incompatible purposes merely because they can technically access it.

17. Data Protection Impact Assessments

A DPIA must be completed before processing likely to result in a high risk to individuals. Examples requiring consideration include systematic monitoring, biometric processing, large-scale special-category data, intrusive AI/profiling, novel surveillance and material changes to filtering/monitoring.

The DPIA will document purpose, necessity, proportionality, risks, controls, consultation where appropriate and residual risk. Where a high residual risk cannot be mitigated, the School will consider whether prior consultation with the ICO is required.

18. Individual rights

Individuals have rights under data-protection law, subject to conditions and exemptions, including access, rectification, erasure, restriction, portability where applicable, objection, rights concerning automated decision-making and withdrawal of consent where consent is relied on.

Requests do not have to mention data-protection law, use a particular form or be sent to the Data Protection Lead. Any staff member receiving a request must forward it immediately.

19. Subject access requests (SARs)

A valid SAR must be handled without undue delay and normally within one month, subject to the statutory rules on extensions, identification, permitted fees and clarification.

The School may ask for clarification only where reasonably required, for example because it holds a large amount of information or the request is unclear. Where the legal test is met, the response clock pauses when clarification is requested and resumes after clarification is received. A requester cannot be forced to narrow a valid request.

The School is required to carry out reasonable and proportionate searches for the requested information. It must be able to justify a decision that further searching would be unreasonable or disproportionate.

Before disclosure, the School will consider third-party information, safeguarding, legal privilege and other applicable exemptions, and will provide information securely in an appropriate format.

20. Requests concerning children

A child's data-protection rights belong to the child. A parent does not automatically have a data-protection right to all personal data about their child solely because they hold parental responsibility.

The School will consider the child's age, maturity, competence, best interests, safeguarding, confidentiality and the authority of the requester. Where appropriate, a competent child may exercise their own rights.

21. Personal data breaches

Staff must report any suspected personal data breach to Chris Sellers / the Headteacher immediately and must not wait to establish whether harm has occurred.

The School will contain the incident, preserve evidence, assess risk, record the decision and take remedial action. Where a breach is likely to result in risk to individuals' rights and freedoms, the ICO must be notified without undue delay and, where feasible, within 72 hours of awareness. Where it is likely to result in high risk, affected individuals must also be informed without undue delay unless an exception applies.

All personal data breaches will be logged, whether or not notified to the ICO.

22. Data-protection complaints - statutory procedure from 2026

The School must provide a clear and accessible process, including an electronic route, for people to complain about how their personal data has been handled. This is a statutory data-protection complaints process and is separate from, though it may run alongside, the School's general Complaints Policy.

The School must acknowledge a data-protection complaint within 30 days. It will make appropriate enquiries, keep the complainant informed of progress where necessary and communicate the outcome without undue delay.

Complaints should be directed to Chris Sellers, Data Protection Lead. The response will explain the outcome and the individual's right to complain to the ICO. The complaint and outcome will be logged for accountability purposes.

23. Sharing and disclosure

Before routine sharing, staff should consider purpose, lawful basis, necessity, proportionality, accuracy, security and whether the recipient is entitled to receive the information.

The School may lawfully share personal data with safeguarding partners, local authorities, police, courts, regulators, professional bodies, health professionals, insurers, advisers, other schools and service providers where necessary and lawful.

Recurring or significant data-sharing arrangements should be documented and a data-sharing agreement used where appropriate.

24. International transfers

Personal data must not be transferred, hosted or made remotely accessible outside the UK unless applicable international-transfer rules are met. Cloud hosting, remote support and subprocessors must therefore be considered during procurement.

25. Retention, archiving and secure disposal

Personal data will be retained only for as long as necessary for its purpose and applicable legal, safeguarding, insurance, contractual or evidential requirements.

The School will maintain an approved master Records Retention Schedule. A litigation, safeguarding, complaint, subject access or regulatory hold may require scheduled deletion to be suspended.

Deletion and disposal must be secure. Staff must not keep shadow copies, personal exports or unofficial archives after the retention need has ended.

26. Safeguarding record retention and transfer

Safeguarding records require particular care and are governed by KCSIE and the School's safeguarding procedures. They must not be deleted simply because a pupil leaves the School if a safeguarding or legal retention reason remains.

When a child transfers school, the child protection file must be transferred securely and separately from the main pupil file in accordance with KCSIE arrangements, with appropriate confirmation of receipt.

27. Staff, recruitment and safeguarding records

Staff records may include recruitment, references, vetting/DBS, right-to-work, contractual, payroll, attendance, performance, grievance, disciplinary, low-level concern, allegation and health/adjustment data where relevant.

Retention periods must distinguish ordinary employment records, low-level concerns and allegations meeting the harm threshold, because safeguarding guidance applies different record-retention rules.

DBS certificate information must be handled in accordance with DBS and data-protection requirements and must not be copied or retained indiscriminately.

28. Financial and payment-card data

Financial details, payroll information, bank data and identity documents require strong security even where they are not special-category data. Where payment-card information is handled, relevant PCI DSS controls will apply. Full card details must not be retained in ordinary emails or School documents.

29. Training and awareness

All staff handling personal data will receive appropriate induction and refresher training covering security, breaches, rights requests, safeguarding information sharing, phishing/cyber risk, AI and approved systems. Role-specific training will be provided for staff handling SARs, HR data, safeguarding records, CCTV/monitoring or high-risk processing.

30. Monitoring, audit and review

The Data Protection Lead will maintain proportionate evidence of compliance, including privacy notices, processing records/data map, processor contracts, DPIAs, breach logs, rights-request logs, complaint logs, training records, key decisions and the retention schedule.

This policy and associated privacy notices will be reviewed at least annually and sooner following significant legal change, a serious breach, new high-risk technology, ICO/DfE guidance changes or a material change in School processing.

Appendix 1 - Staff Privacy Notice

This notice applies to employees, applicants, contractors, visiting/peripatetic workers, casual and temporary workers, volunteers and the Director. It explains how The Mount School uses personal data in connection with recruitment, work and engagement.

Information we may collect

- identity and contact details, including emergency and next-of-kin information;
- application, education, qualification, reference and employment history;
- right-to-work, DBS, safeguarding, suitability and online-search information where lawful;
- payroll, tax, pension, bank and benefit information;
- attendance, sickness, performance, training and professional-development records;
- work product, communications, system/security logs and records created in the course of duties;
- photographs, CCTV and security information;
- health, disability and reasonable-adjustment information where necessary;
- equality-monitoring and other special-category data where lawfully processed;
- disciplinary, grievance, complaint, allegation and low-level-concern records where relevant.

Purposes and lawful bases

Purposes include recruitment and pre-contract steps, performance of employment/engagement contracts, payroll and benefits, legal and regulatory compliance, safeguarding, health and safety, workforce management, training/performance, security, investigation of concerns, defence of legal claims and provision of education. The lawful basis and any additional special-category/criminal-offence condition will depend on the specific processing activity.

Who information may be shared with

Recipients may include payroll/pension providers, HMRC, DBS, referees, professional/regulatory bodies, insurers/advisers, IT and other processors, occupational health, safeguarding agencies, police, courts and other authorities where lawful.

Retention, rights and complaints

Staff information is retained in accordance with the School's master retention schedule and safeguarding requirements. Staff may exercise applicable data-protection rights and may complain to the School using the statutory data-protection complaints route and to the ICO.

Appendix 2: Prospective Family, Pupil and Parent Privacy Notice

Who this notice applies to

This privacy notice applies to prospective pupils and their parents/carers from the point of first enquiry or application, as well as current pupils and their parents/carers.

The Mount School collects and uses personal data during enquiries, visits, taster days and the admissions process, and throughout a child's time at the School.

How we use personal data

The School may use pupil and parent/carer personal data to:

- respond to enquiries and requests for information;
- provide prospectuses and admissions information;
- arrange visits, tours, open days and taster sessions;
- process applications, registrations and admissions;
- provide education and care;
- safeguard children and support their welfare;
- meet legal and regulatory duties;
- communicate with prospective and current families;
- administer fees and payments;
- support SEND, disability, medical and dietary needs;
- assess progress and maintain educational records;
- manage attendance and behaviour;
- organise clubs, visits and activities;
- maintain security and operate the School effectively.

Information we may collect and hold

Depending on the stage of enquiry, application or attendance, this may include:

- names, addresses, contact details and family information;
- enquiry, application, admissions and registration information;
- information provided during visits and taster sessions;
- previous school or nursery information and educational records;
- attendance, assessments, reports and learning information;
- SEND, disability, health, allergy, dietary and intimate-care information where relevant;
- safeguarding, pastoral, behaviour and welfare records;
- photographs, video, audio and CCTV;
- online-system, filtering, monitoring and device information where relevant;
- trip, club and activity information;
- fee, payment and account information;
- communications, complaints, rights requests and consent or preference records.

Lawful basis for processing

The School will only process personal data where it has a lawful basis to do so. Depending on the purpose, this may include taking steps at the request of a parent/carer before entering into a contract, performance of a contract, compliance with a legal obligation, the School's legitimate interests, vital interests or consent where appropriate.

Where special category data is processed, such as health, disability or other sensitive information, the School will also identify an appropriate additional legal condition.

Consent will only be relied upon where it is the appropriate lawful basis and may be withdrawn where applicable.

Sharing information

The School will only share personal data where there is a lawful and necessary reason to do so.

Information may be shared, where appropriate, with parents/carers, other schools or nurseries, local authorities, safeguarding partners, health professionals, police, courts, regulators and inspectors, assessment bodies, activity providers, insurers, professional advisers and contracted service providers.

Safeguarding information may be shared without consent where necessary to protect a child.

The School does not sell personal data.

Retention

Personal data is retained only for as long as it is reasonably required for the purpose for which it was collected and to meet applicable legal, safeguarding, contractual, insurance and regulatory requirements.

Information relating to enquiries or applications which do not result in a child joining the School will be retained in accordance with the School's approved Records Retention Schedule.

Keeping in touch with prospective families

Where permitted by law, the School may contact prospective families about their enquiry, application, visits, availability of places and related admissions matters.

Where separate consent is required for marketing communications, families will be given a clear choice and may change their preferences or withdraw consent at any time.

Your rights

Prospective pupils, pupils and parents/carers may exercise applicable rights under data-protection law, including rights relating to access, rectification, erasure, restriction, objection and withdrawal of consent where consent is relied upon.

A parent's authority to exercise rights on behalf of a child will depend on the circumstances, including the child's age, competence and best interests.

Questions, requests or concerns about personal data should be directed to:

Chris Sellers
Data Protection Lead
The Mount School
3 Bingham Road
Edgerton
Huddersfield
HD2 2AP
Email: info@themount.org.uk
Telephone: 01484 426432

Data-protection complaints will be handled in accordance with section 22 of this policy. Individuals also have the right to raise a concern with the Information Commissioner's Office.

Appendix 3 - Personal data breach immediate response

- STOP / CONTAIN: recall messages where possible, revoke links, recover documents/devices and follow IT instructions.
- REPORT IMMEDIATELY to Chris Sellers / Headteacher. Do not wait for proof of harm.
- PRESERVE evidence and relevant logs.
- RECORD what data, whose data, volume, protections and likely consequences.
- ASSESS risk, including safeguarding, fraud, confidentiality, discrimination and distress.
- DECIDE ICO and affected-person notification; record rationale.
- REMEDIATE and REVIEW lessons learned.

Appendix 4 - Subject access request checklist

- Record the date received and exact wording.
- Forward immediately to the Data Protection Lead.
- Verify identity/authority only as reasonably necessary.
- Clarify only where reasonably required; record any lawful pause.
- Identify relevant systems, custodians, paper files, email and processors.
- Carry out reasonable and proportionate searches.
- Review third-party information and exemptions, especially safeguarding.
- Redact and quality-check securely.
- Respond within the statutory deadline and retain the search/decision audit trail.

Appendix 5 - Data-protection complaint record

Field	Record
Complainant / contact	
Date received	
Acknowledgement date - within 30 days	
Issue complained of	
Related SAR / safeguarding / HR / general complaint?	
Person handling complaint	
Enquiries and evidence	
Progress update(s)	
Outcome and remedial action	

Field	Record
Outcome date	
ICO right explained	Yes / No
Learning / policy change	

Appendix 6 - DPIA screening prompt

- Is this a new system/process or significant change?
- Does it involve children or vulnerable people?
- Does it involve special-category or criminal-offence data?
- Does it involve systematic monitoring, CCTV, filtering/monitoring or location tracking?
- Does it involve AI, profiling or significant automated decisions?
- Is the technology novel, intrusive or difficult for individuals to understand?
- Will information be transferred internationally or shared widely?
- Could misuse significantly affect rights, safety, education, employment or opportunities?
- Can the purpose be achieved with less personal data?
- If high risk is likely, complete a full DPIA before implementation.

Appendix 7 - Records retention schedule framework

Record class	Retention basis / rule
Safeguarding / child protection	KCSIE/safeguarding requirements and case need; secure transfer where required
Pupil educational records	Education/legal/contractual need and approved master retention schedule
SEND / medical / allergy	Purpose, legal claims, safeguarding and medical requirements
Attendance / admissions	Applicable education/regulatory requirements
Complaints	Independent School Standards, EYFS, data-protection, legal and contractual need
Staff personnel / payroll	Employment, tax, pension, limitation and contractual requirements
Recruitment	Recruitment/equality/claims need; defined retention period
Staff safeguarding allegations	KCSIE harm-threshold retention rule
Low-level concerns	KCSIE low-level-concern retention rule
CCTV / monitoring	Defined operational period unless preserved for incident/investigation
Accident / H&S	Health and safety, RIDDOR, insurance and claims requirements
Financial / accounting	Tax, accounting and contractual requirements
Data-protection requests / breaches / complaints	Accountability, limitation and regulatory need

The School must populate and approve exact retention periods in its master Records Retention Schedule using current legal, safeguarding and recognised sector guidance. This framework deliberately avoids inventing a universal period where the correct period depends on the record and context.

Appendix 8 - Data Protection Lead / DPO status check

- Has the School documented whether it is legally required to appoint a statutory DPO?
- If not legally required, has it decided whether to use the formal title DPO voluntarily?
- If using the formal DPO title, does the appointee have independence, sufficient expertise/resources and direct access to highest management?
- Does the appointee have any role which determines purposes and means of processing and could create a conflict of interest?
- If a conflict exists, should the School retain a Data Protection Lead internally and appoint an independent external DPO/adviser instead?
- Are contact details and ICO registration details accurate and current?