MOUNT KELLY
Boarding and Day School
Boys and Girls, Aged 4-18

Data Protection Policy

This policy applies to all pupils including those in the EYFS

Reviewed	September 2026
Next Review	September 2027
Owner	Privacy Officer

Date of Review	Author	Page / Para	Synopsis of Amendment
Jun 18	S Webber		Policy re-written in line with GDPR implementation
Jul 18	S Webber	Page 3	Insertion of footnote to Foundation background.
26/10/2020	N Harvey	Throughout	Updated policy owner to Privacy Officer. Removed reference to Bursar.
01/01/2021	N Harvey	Page 4	Updated background information following UK adoption of EU GDPR.
April 2026	N Harvey	Section 8 and 9.	Added further detail on Data Impact Assessments and Data Retention and Disposal
June 2026	N Harvey	Added section 7	Added Data Protection Complaints effective from 19 June 2026.

1. Background

Data protection is an important legal compliance issue for Mount Kelly.

During the course of the business activities we will collect, store and process personal data (sometimes sensitive in nature) about staff, pupils, their parents, suppliers and other third parties (in a manner more fully detailed in the Privacy Notices). It is therefore an area where all staff have a part to play in ensuring we comply with and are mindful of our legal obligations, whether that personal data is sensitive or routine.

While the Data Protection (2018) law sets out useful legal grounds in this area, in most ways the law is strengthening the rights of individuals and placing tougher compliance obligations on organisations including schools that handle personal information. The Information Commissioner's Office (ICO) is responsible for enforcing data protection law and has powers to act for breaches of the law.

Those who are involved in the processing of personal data are obliged to comply with this policy when doing so. Accidental breaches will happen and may not be a disciplinary issue, but any breach of this policy may result in disciplinary action. Data breaches may also need to be reported to regulators.

This policy sets out the expectations and procedures with respect to processing any personal data collected from data subjects (e.g. including parents, pupils, governors, employees and alumni).

Key data protection terms used in this data protection policy are:

- **Data controller** – an organisation that determines the purpose and means of the processing of personal data. For example, the School is the controller of pupils' personal information. As a data controller, we are responsible for safeguarding the use of personal data.
- **Data processor** – an organisation that processes personal data on behalf of a data controller, for example a payroll provider or other supplier of services.
- **Personal data breach** – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- **Personal information (or personal data):** any information relating to a living individual (a data subject), including name, identification number, location or online identifier such as an email address. Note that personal information created in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings) is still personal data and regulated by data protection laws, including the GDPR. Note also that it includes expressions of opinion about the individual or any indication of someone's intentions towards that individual.
- **Processing** – virtually anything done with personal information, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it.
- **Special categories of personal data** – data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and medical conditions, sex life or sexual orientation, genetic or biometric data used to identify an individual. There are also separate rules for the processing of personal data relating to criminal convictions and offences.

2. Privacy Officer

The Privacy Officer is supported by the Assistant Privacy Officer, who will endeavour to ensure that all personal data is processed in compliance with this Policy and the principles of UK data protection. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Privacy Officer.

3. The Principles

The ICO sets out seven principles relating to the processing of personal data which must be adhered to by data controllers (and data processors). These require that personal data must be:

1. Processed **lawfully, fairly** and in a **transparent** manner;
2. Collected for **specific and explicit purposes** and only for the purposes it was collected for;
3. **Relevant** and **limited** to what is necessary for the purposes it is processed;
4. **Accurate** and kept **up to date**;
5. **Kept for no longer than is necessary** for the purposes for which it is processed; and
6. Processed in a manner that ensures **appropriate security** of the personal data.
7. The 'accountability' principle also requires that personal data is processed in a fair and legal manner and that the School is able to demonstrate compliance with the data protection principles. This involves, among other things:
    - keeping records of our data processing activities, including by way of logs and policies;
    - documenting significant decisions and assessments about how we use personal data; and
    - generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how our Privacy Notices were updated, how and when data protection consents were collected from individuals, how breaches were dealt with, etc.

4. Lawful grounds for data processing

Under data protection principles there are several different lawful grounds for processing personal data. One of these is consent. However, because the definition of what constitutes consent has been tightened (and the fact that it can be withdrawn by the data subject) it is generally considered preferable to rely on another lawful ground where possible.

One of these alternative grounds is 'legitimate interests', which is the most flexible basis for processing. However, it does require transparency and a balancing assessment between the rights of the individual and the interests of the Controller. It can be challenged by data subjects and also means

the Controller is taking on extra responsibility for considering and protecting people's rights and interests. The legitimate interests are set in the Privacy notice.

Other lawful grounds include:

- compliance with a legal obligation, including in connection with employment and diversity;
- contractual necessity, e.g. to perform a contract with staff or parents;
- Special categories of personal data (including health, safeguarding and wellbeing information) are processed only where a specific condition under Article 9 of the UK GDPR and Schedule 1 of the Data Protection Act 2018 applies. These include, where relevant, obligations under employment law, safeguarding and child protection, medical purposes, substantial public interest, or where the data subject has given explicit consent.

5. Headline responsibilities of all staff

Record-keeping

It is important that personal data held is accurate, fair and adequate. You are required to inform the relevant member of staff if you believe that *your* personal data is inaccurate or untrue or if you are dissatisfied with the information in any way. Similarly, it is vital that the way you record the personal data of others – in particular colleagues, pupils and their parents – is accurate, professional and appropriate.

Staff should be aware of the rights set out below, whereby any individuals about whom they record information in emails and notes may have the right to see that information. This absolutely must not discourage staff from recording necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils, in accordance with other policies, and grounds may sometimes exist to withhold these from such requests. However, the starting position is to record every document or email in such a way that you would be able to stand by it if the person about whom it was recorded were to see it.

All staff must complete GDPR training and refresher sessions. The use of personal emails for school business is not permitted.

Data handling

All staff have a responsibility to handle the personal data which they come into contact with fairly, lawfully, responsibly and securely and in accordance all relevant policies and procedures. In particular, there are data protection implications across a number of areas such as safeguarding and IT security, so all staff should read and comply with the following policies:

- ICT Acceptable Use Policy
- Mobile Devices Policy
- Guidelines for Staff Social Media Use.

Responsible processing also extends to the creation and generation of new personal data / records, as above, which should always be done fairly, lawfully, responsibly and securely.

Data sharing occurs when personal data is shared with outside organisations e.g. Department for Education (DfE), NHS, Exam boards and educational platforms, Police or Social Services.

Avoiding, mitigating and reporting data breaches

One of the key obligations is on reporting personal data breaches. Data controllers must report certain types of personal data breach (those which risk an impact to individuals) to the ICO within 72 hours.

In addition, data controllers must notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms. In any event we must keep a record of any personal data breaches, regardless of whether we need to notify the ICO. If you become aware of a personal data breach you must notify the Privacy Officer, the Assistant Privacy Officer or a member of the Senior Leadership Team immediately. If staff are in any doubt as to whether or not you should report something, it is always best to do so. A personal data breach may be serious, or it may be minor, and it may involve fault or not, but it must be reported.

A failure to report could result in significant exposure, and for those affected, and could be a serious disciplinary matter whether under this Policy or the staff member's contract.

Care and data security

More generally, we require all staff to remain conscious of the data protection principles (see section 3 above), to attend any training we require them to, and to use their best efforts to comply with those principles whenever they process personal information. Data security is not simply an online or digital issue but one that affects daily processes: filing and sending correspondence, notably hard copy documents. Staff should always consider what the most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

We expect all those with management / leadership responsibilities to be particular champions of these principles and to oversee the swift reporting of any concerns about how personal information is used to the Privacy Officer, and to identity the need for (and implement) regular staff training.

6. Rights of Individuals

In addition to the responsibility when processing personal data, individuals have certain specific rights, perhaps most significantly that of access to their personal data held by a data controller. This is known as the 'subject access right' (or the right to make 'subject access requests'). Such a request must be dealt with promptly, and usually within one calendar month subject to permitted extensions for complex requests and does not need any formality, nor to refer to the correct legislation. If you become aware of a subject access request (or indeed any communication from an individual about their personal data), you must tell the Privacy Officer as soon as possible.

Individuals also have legal rights to:

- require us to correct the personal data we hold about them if it is inaccurate;

- request that we erase their personal data (in certain circumstances);
- request that we restrict our data processing activities (in certain circumstances);
- receive from us the personal data we hold about them for the purpose of transmitting it in a commonly used format to another data controller;
- object, on grounds relating to their particular situation, to any of our particular processing activities where the individual feels this has a disproportionate impact on them; and
- object to automated individual decision-making, including profiling (where a significant decision is made about the individual without human intervention), and to direct marketing, or to withdraw their consent where we are relying on it for processing their personal data.

Except for the final bullet point, none of these rights for individuals are unqualified and exceptions may well apply. In any event, however, if you receive a request from an individual who is purporting to exercise one or more of their data protection rights, you must tell the Privacy Officer as soon as possible.

7. Data Protection Complaints

From 19 June 2026, individuals have a statutory right to raise a complaint with the School regarding the handling of their personal data. The School is committed to handling such complaints promptly, fairly, and transparently.

Complaints may be made by any individual whose personal data is processed by the School (including pupils, parents, staff, and other stakeholders), and may relate to any aspect of data protection, including the use, accuracy, retention, sharing, or security of personal data.

The School will:

- Provide clear and accessible methods for individuals to submit a data protection complaint;
- Acknowledge receipt of a complaint within 30 days;
- Investigate the complaint without undue delay, making appropriate enquiries where necessary;
- Keep the individual informed of progress where appropriate; and
- Communicate the outcome of the complaint clearly and without undue delay.

Responsibility for managing data protection complaints sits with the Privacy Officer, who will maintain a record of all complaints received and their outcomes in accordance with the School's accountability obligations.

Where an individual is dissatisfied with the outcome of their complaint, they retain the right to escalate the matter to the Information Commissioner's Office (ICO).

All staff must ensure that any complaint or concern relating to personal data is referred to the Privacy Officer as soon as possible.

8. Data Security: online and digital

We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Therefore, no member of staff is permitted to remove personal data from work premises, whether in paper or electronic form and wherever stored, without the prior consent of the Head or Privacy Officer, except where otherwise permitted by this policy or associated procedures. Where a member of staff is permitted to take electronic data offsite it will need to be encrypted. All Foundation issued portable devices are encrypted and acceptable for temporary storage, such as for a trip or leave, but must be migrated over to appropriate storage or deleted as soon as the trip or leave is complete.

The use of personal email accounts or unencrypted personal devices for business is not permitted. Unless unavoidable for personal data must not be downloaded onto personal devices. If essential, that data must not be stored on personal devices for any length of time and must be deleted as soon as it is no longer required to be held. Such data must be securely deleted, by being deleted from the recycle bin also.

9. Data Protection and Impact Assessments

The School will carry out a Data Protection Impact Assessment (DPIA) where any processing of personal data is likely to result in a high risk to the rights and freedoms of individuals. This includes, but is not limited to, the introduction of new technologies, large-scale processing of special category data, systematic monitoring, or the use of biometric or safeguarding-related systems.

DPIAs will be completed prior to the commencement of such processing and reviewed by the Privacy Officer. Records of DPIAs will be retained in accordance with accountability obligations.

10. Data Retention and Disposal

Personal data will be retained only for as long as necessary for the purpose for which it was collected, in accordance with the School's Retention Schedule. Once personal data is no longer required, it will be securely deleted or destroyed. Hard-copy records will be securely shredded and electronic records permanently deleted in accordance with IT security procedures.

11. Summary

It is in everyone's interests to get data protection right and to think carefully about data protection issues: this means handling all personal information with which you come into contact fairly, lawfully, securely and responsibly.

A good rule of thumb here is to ask yourself questions such as:

- Would I be happy if my own personal information were being used (for example, shared with a third party) in the way I am proposing? Would I expect it?
- Would I wish to stand by how I have recorded this information in an email or official record if the person concerned was able to see it?
- What would be the consequences of my losing or misdirecting this personal data?

Data protection law is therefore best seen not as oppressive red tape, or a reason not to do something necessary or important, but a code of useful and sensible checks and balances to improve how we handle and record personal information and manage our relationships with people. This is an important part of our culture and all its staff and representatives need to be mindful of it.

Appendix A: Data Retention

All retention periods set out below represent minimum retention periods. Records must not be destroyed where they are relevant to ongoing or reasonably foreseeable safeguarding concerns, complaints, litigation, employment disputes, regulatory enquiries, or statutory investigations.

Type of Record/Document	**Suggested Retention Period**
Emails on the server Pupil email account	Delete within 1 year of leaving the School, subject to preservation of any emails relevant to safeguarding, complaints, or disputes.
Staff emails	Routine emails may be deleted after 2 years, subject to relevance. Accounts to be deleted within 1 year of leaving, but emails relevant to safeguarding, employment, complaints, or litigation must be retained for a minimum of 6 years post-employment. Emails must not be deleted where they are subject to a legal hold, ongoing investigation, or reasonably foreseeable dispute.
School specific records	
Registration documents of School	Permanent (or until closure of the school)
Attendance Register	6 years from last date of entry, then securely archived or destroyed.
Minutes of Governors' meetings	Permanent (minimum 10 years where permanent archiving is not practicable).
Annual curriculum	Curriculum plans: 3 years from end of academic year. Other class records (marks, assignments, timetables): 1 year.
Pupil Records	
Admissions:application forms, assessments, records of decisions	25 years from date of birth (or 7 years from leaving, whichever is later). Up to 1 year after decision.
Student immigration records	Duration of sponsorship plus minimum 1 year, or longer as required by UKVI guidance.

Examination results (external or internal)	7 years from pupil leaving school
Pupil file including: • Pupil reports and performance records • Pupil medical records (*not accidents*)	25 years from date of birth, subject to safeguarding override.
Special educational needs records	Date of birth + up to 35 years, subject to individual risk assessment.
<u>Safeguarding</u> Policies, procedures and insurance	Permanent archive of historic versions.
DBS disclosure certificates (if held)	No longer than 6 months from recruitment decision. Record of checks retained on SCR/personnel file only.
Accident / Incident reporting	Retain for as long as any living individual may bring a claim. Files to be reviewed periodically with oversight from DSL and Privacy Officer.
Child Protection files and specific records of child sexual abuse	If a referral has been made / social care have been involved / child has been subject of a multi-agency plan; or if any risk of future claim(s): 75 years.
Video recordings of meetings	3–6 months, or shorter where reviewed promptly by the DSL. Must not be retained beyond safeguarding purpose and must be referenced in Privacy Notices.
<u>Corporate Records (e.g. where schools have trading arms)</u>	
Certificates of Incorporation	Permanent (or until dissolution of the company)
Minutes, Notes and Resolutions of Boards or Management Meetings	Minimum 10 years
Shareholder resolutions	Minimum 10 years
Register of Members/Shareholders	Permanent (minimum 10 years for ex members/shareholders)
Annual reports	Minimum 6 years
<u>Accounting Records</u>	
Accounting records (*normally taken to mean records which enable a company's accurate financial position to be*	Minimum 6 years from end of financial year (or longer if required for tax purposes).

ascertained & which give a true and fair view of the company's financial state)	Minimum 6 years for UK charities (and public companies) from the end of the financial year in which the transaction took place Internationally: can be up to 20 years depending on local legal/accountancy requirements
Tax returns	Minimum 6 years
VAT returns	Minimum 6 years
Budget and internal financial reports	Minimum 3 years
<u>Contracts and Agreements</u>	
Signed or final/concluded agreements (*plus any signed or final/concluded variations or amendments)*	Minimum 7 years from completion of contractual obligations or term of agreement, whichever is the later
Deeds (or contracts under seal)	Minimum 13 years from completion of contractual obligation or term of agreement
<u>Intellectual Property Records</u>	
Formal documents of title (trade mark or registered design certificates; patent or utility model certificates)	Permanent (in the case of any right which can be permanently extended, eg trade marks); otherwise expiry of right plus minimum of 7 years.
Assignments of intellectual property to or from the school	As above in relation to contracts (7 years) or, where applicable, deeds (13 years).
IP / IT agreements (including software licences and ancillary agreements e.g. maintenance; storage; development; coexistence agreements; consents)	Minimum 7 years from completion of contractual obligation concerned or term of agreement
<u>Employee/Personnel Records</u>	
Single Central Record of employees	Keep a permanent record that mandatory checks have been undertaken (but do <u>not</u> keep DBS certificate information itself: 6 months as above)
Contracts of employment	7 years from effective date of end of contract
Employee appraisals or reviews	Duration of employment plus minimum of 7 years

Staff personnel file	As above, but do not delete any information which may be relevant to historic safeguarding claims
Payroll, salary, maternity pay records	Minimum 6 years
Pension or other benefit schedule records	Potentially permanent (ie lifetimes of those involved), depending on nature of scheme
Job application and interview/rejection records (unsuccessful applicants)	Minimum 3 months but no more than 1 year (as CVs will rapidly be out of date)
Staff immigration records (Right to work, etc.)	Minimum 2 years from end of employment
Tier 2 migrant worker sponsor records	Minimum 1 year from end of employment
Health records relating to employees	7 years from end of employment, unless the records relate to occupational health, hazardous substances, or long-latency conditions, in which case significantly longer retention (e.g. 40 years) may be required.
Records of low-level concerns about adults	At least until end of employment (as recommended by KCSIE), then subject to review for relevance: e.g. 7 years from end of employment if they have ongoing relevance for employment claims, longer if necessary for safeguarding purposes / claims.
Insurance Records	
Insurance policies (will vary – private, public, professional indemnity)	Duration of policy (or as required by policy) plus a period for any run-off arrangement and coverage of insured risks: ideally, until it is possible to calculate that no living person could make a claim.
Correspondence related to claims/ renewals/ notification re: insurance	Minimum 7 years (*but this will depend on what the policy covers and whether e.g. historic claims may still be made*)
Environmental Health and Data	Minimum 6 years from date of accident, with longer retention where the nature of the injury, exposure, or safeguarding issues indicate potential future claims 10 years from date of last entry
Maintenance logs	10 years from date of last entry
Accidents to children	25 years from birth (longer for safeguarding)

Accident at work records (staff) Staff use of hazardous substances Covid-19 risk assessments, consents etc. (*for now: this to be subject to further review*)	Minimum 6 years from date of accident, with longer retention where the nature of the injury, exposure, or safeguarding issues indicate potential future claims Minimum 7 years from end of date of use, or longer where required by health and safety legislation (e.g. COSHH) or where long-latency conditions may arise. Retain for now legal paperwork (consents, notices, risk assessments) but not individual test results
Risk assessments (carried out in respect of above)	7 years from completion of relevant project, incident, event or activity.
Art.30 UK GDPR records of processing activity (ROPAs), data breach records, data protection impact assessments	No limit (as long as no personal data held), but must be kept up-to-date, accurate and relevant.