



Reviewed: September 2025
Next Review: September 2026
Policy Owner: Headmaster
Approved by: Pete Gosling, Governor

DATA PROTECTION POLICY

Background

Data protection is an important legal compliance issue for Moor Park School. During the course of the School's activities it collects, stores and processes personal data (sometimes sensitive in nature) about staff, pupils, their parents, suppliers and other third parties (as detailed in the School's Privacy Notice).

This processing is governed by the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. These laws strengthen the rights of individuals and place obligations on organisations, including schools, to process personal data fairly, lawfully and transparently.

In the context of safeguarding obligations, the school has a heightened duty to ensure that the personal data of pupils is handled responsibly and securely at all times.

The Information Commissioner's Office (ICO) is responsible for enforcing data protection law. Those who are involved in the processing of personal data are obliged to comply with this policy. Accidental breaches will happen and may not be a disciplinary issue, but any breach of this policy may result in disciplinary action.

This policy sets the school's expectations and procedures with respect to processing any personal data we collect from data subjects (eg including parents, pupils, employees).

Key protection terms used in this policy are:

1. 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.
2. Data processor – an organisation that processes personal data on behalf of a data controller, for example a payroll provider or other supplier of services.
3. Personal data breach – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
4. 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.
5. Processing – virtually anything done with person information, including obtaining it 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.
6. 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, gender or sexual orientation,



genetic or biometric data used to identify an individual. There are also separate rules for the processing of personal data relation to criminal convictions and offences.

Data Protection Officer

The School has appointed the Headteacher, as the Data Protection Officer (DPO). The DPO will endeavour to ensure that all personal data is processed in compliance with this policy and the principles of the GDPR. 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 DPO.

Data Protection Principles

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

- Processed lawfully, fairly and in a transparent manner;
- Collected for specific and explicit purposes and only for the purposes it was collected for;
- Relevant and limited to what is necessary for the purposes it is processed;
- Accurate and kept up to date;
- Kept for no longer than is necessary for the purposes for which it is processed; and
- Processed in a manner that ensures appropriate security of the personal data.

The GDPR's 'accountability' principle also requires that the school not only processes personal data in a fair and legal manner, but that we are also able to demonstration that our processing is lawful. This involves, amongst 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-a vis data protection and privacy matters, including for example when and how our Privacy Notice was updated, how and when data protection consents were collected from individuals, how breaches were dealt with etc.

Lawful Bases for Processing

The School processes personal data under the following lawful bases:

- Contract: to fulfil obligations with staff and parents
- Legal obligation: including safeguarding, health and safety, and regulatory requirements
- Legitimate interests: to operate the School effectively, provided these are not overridden by individual rights
- Vital interests: to protect individuals in emergencies
- Consent: where required, particularly for certain uses of images or optional activities

Special category data (.g health, safeguarding information) is processed under additional lawful conditions, including substantial public interest and safeguarding purposes.

Processing of Pupil Data

The School processes pupil data for educational provision, pastoral care, safeguarding, and administration.



In some circumstances, the School may rely on parental consent, particularly for younger pupils, although it will usually rely on other lawful bases such as legal obligation or legitimate interests.

Safeguarding considerations may override certain data protection rights where necessary to protect a child.

Data Retention

The School maintains a Data Retention Schedule which sets out how long different categories of personal data are kept. Personal data will not be retained for longer than necessary. Safeguarding records may be retained for extended periods in line with statutory guidance.

Data Sharing

The School may share personal data with third parties where necessary, including:

- Local authorities and safeguarding bodies
- Examination boards
- Regulatory authorities
- IT service providers

All sharing is carried out in accordance with data protection law and appropriate safeguards.

Data Protection Impact Assessments (DPIAs) and Risk Assessment

The School will carry out DPIAs or a risk assessment where processing is likely to result in a high risk to individuals, such as the use of CCTV or new technologies. Please refer to Appendix I (example risk assessment).

Staff Responsibilities

It is important that personal data held by the School is accurate, fair and adequate. You are required to inform the School 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 on School business 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 the School's other policies, and grounds may sometimes exist to withhold these. 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 was to see it.

All staff must:

- Handle and create personal data securely, appropriately, fairly, lawfully, responsibly and in accordance with the staff handbook and all relevant School policies;
- Report data breaches immediately to the DPO. A personal data breach may be serious, or it may be minor, and it may involve fault or not, but the School always needs to know about them to make a decision;
- Follow all relevant policies (more specifically Child Protection, Anti-Bullying, IT – Acceptable Use, CCTV, E-Safety, Mobile Phones and Other Mobile Devices, Bring your Own Device policies).



Data Breaches

The School will report notifiable breaches to the ICO within 72 hours where required and will inform affected individuals where there is a high risk.

All breaches must be reported to the DPO immediately. As stated earlier, the School may not need to treat the incident itself as a disciplinary matter, but a failure to report could result in significant exposure for the School, and for those affected, and could be a serious disciplinary matter whether under this Policy or the staff member's contract.

Individual Rights

Individuals have the right to:

- Access their personal data (Subject Access Request – responded to within one month)
- Rectification
- Erasure (in certain circumstances)
- Restriction of processing
- Data portability
- Object to processing

If staff receive a request from an individual who is purporting to exercise one or more of their data protection rights, staff must inform the DPO.

The school may apply exemptions, particularly where safeguarding is concerned.

Security

The School implements appropriate technical and organisational measures to protect personal data, including secure systems and controlled access.

Use of personal devices and personal email for School business is prohibited unless authorised.

Privacy Notices

The School provides Privacy Notices to pupils, parents and staff explaining how their data is used.

Summary

All staff must ensure personal data is handled lawfully, securely and responsibly at all times.



APPENDIX 1
RISK ASSESSMENT FOR: Risk of Personal Data Leakage
ASSESSORS: Headmaster and Bursar
DATE: September 2025

Those at risk – Children, Staff, parents and visitors.

Purpose of this risk assessment: This assessment considers the risk of accidental, unlawful or unauthorised disclosure, loss or access to personal data held by the school. The school processes personal data relating to pupils, parents, staff, governors, volunteers and contractors. As a public authority and data controller, the school must comply with the UK GDPR and Data Protection Act 2018.

Scope of this risk assessment: Electronic records held on school systems, paper records/files, email communications, cloud systems/MIS/learning platforms, remote working arrangements, third party processors and suppliers, staff handling of personal information.

HAZARD	EXISTING CONTROL MEASURES	FURTHER CONTROL MEASURES
Leak of personal data (names, addresses, contact details, attendance and assessment records, safeguarding information, medical data, staff and payroll records and images)	Data Protection Policy, staff confidentiality clauses, annual GDPR protection training, password standards, restricted access permissions, secure disposal/shredding protocols, locked offices and filing systems, incident reporting process, published Privacy Notice.	2FA, encryption as required, regular review of access to safeguarding and SEND systems, refresher training for all staff, secure parent communication portal.
Remedial action in the event of a data leak.	Incident reported immediately to Headteacher (DPO), contain measures implemented as required, risk to individuals assessed, decision made on ICO notification within 72 hours where required, individuals informed where a high risk exists, lessons learned recorded.	