

Data Protection Policy

Reviewed by: Bursar, June 2026
Approved by: HSRM Committee June 2026

Next review by: June 2027



1 Introduction

- 1.1 This policy sets out how the School expects staff and others working on its behalf to handle Personal Data in accordance with UK data protection law. It explains the School's approach to handling Personal Data, the responsibilities of staff when using Personal Data in the course of their work, and the rights individuals have in relation to their information, including the right to access a copy of the Personal Data the School holds about them.
- 1.2 This policy is distinct from the School's Privacy Notices, which explain how Personal Data is collected and used in relation to individuals.
- 1.3 The Information Commissioner's Office (ICO) is the UK regulator responsible for enforcing data protection law and has powers to investigate complaints and take action where breaches occur.

2 Lawful treatment of data

- 2.1 The School collects, stores and process Personal Data about staff, pupils, parents, governors, volunteers, suppliers and other third parties. The School recognises that handling Personal Data properly is important to maintain confidence in the School and to ensure that it meets its legal obligations. All Personal Data must only be processed where there is a valid lawful basis under UK data protection law, and staff must ensure they understand the reason the data is being used.
- 2.2 The School relies on a number of lawful bases under UK GDPR, including:
 - consent (where appropriate);
 - performance of a contract;
 - compliance with a legal obligation;
 - protection of vital interests;
 - performance of a task carried out in the public interest; and
 - legitimate interests.

The appropriate lawful basis will depend on the nature and purpose of the processing.

3 Other policies

- 3.1 This policy should be read alongside the following:
 - Acceptable Use of ICT for Staff Policy;
 - Acceptable Use of ICT for External Coaches
 - Biometric Information Notice
 - Information Security Policy;
 - Privacy Notice for Pupils and Parents;
 - Privacy Notice for Staff; and
 - Taking, Storing and Using Images of Children Policy.

4 Scope and Application

- 4.1 This policy applies to all staff and others working for or on behalf of the School, whether paid or unpaid, including employees, governors, contractors, agency staff, and volunteers.
- 4.2 All staff must comply with this policy when processing Personal Data on the School's behalf.

- 4.3 Any breach of this policy may result in disciplinary action, including dismissal in serious cases.

5 Roles and Responsibilities

- 5.1 The Bursar, supported by the Head of Legal and Compliance, is responsible for overseeing compliance with this policy. Any queries concerning data protection matters should be raised with the Bursar or Head of Legal and Compliance.

6 Personal Data

- 6.1 Personal Data means any information relating to a living individual who can be identified, either directly or indirectly.
- 6.2 Personal Data is processed throughout School operations. Staff must treat any information relating to an identifiable individual as Personal Data unless confirmed otherwise.
- 6.3 Examples of where Personal Data may be held include (this list is not exhaustive):
- 6.3.1 on a computer database such as iSAMS;
 - 6.3.2 in electronic files on the school network or in Google Drive;
 - 6.3.3 on a paper file, such as the pupil files;
 - 6.3.4 a report about a child protection or safeguarding incident;
 - 6.3.5 a staff disciplinary record;
 - 6.3.6 School newsletters;
 - 6.3.7 photographs and videos of pupils;
 - 6.3.8 a register or contract of employment;
 - 6.3.9 contact details of pupils, parents and staff;
 - 6.3.10 financial records;
 - 6.3.11 information on a pupil's performance;
 - 6.3.12 health records; and
 - 6.3.13 email correspondence.
- 6.4 Staff must not assume that Personal Data is limited to formal records and must consider all formats, including informal communications.
- 6.5 **Special Category Personal Data:** is personal data defined under Article 9 UK GDPR which is more sensitive and requires a higher level of protection. These include:
- 6.5.1 racial or ethnic origin;
 - 6.5.2 political opinions;
 - 6.5.3 religious or philosophical beliefs;
 - 6.5.4 trade union membership;
 - 6.5.5 data concerning health;
 - 6.5.6 data concerning a person's sex life or sexual orientation;
 - 6.5.7 biometric data where used for identification purposes.

- 6.6 Genetic data Special Category Personal Data must only be processed where:
- 6.6.1 there is a valid lawful basis under UK GDPR; and
 - 6.6.2 an additional condition for processing applies due to the sensitive nature of the data.
- 6.7 Staff must not process Special Category Personal Data unless they are authorised to do so and are satisfied that it is necessary for a clear and legitimate purpose. Staff must seek advice from the Bursar or Head of Legal and Compliance if they are unsure about processing Special Category Personal Data.
- 6.8 **Other Sensitive Personal Data:** The School also processes other types of Personal Data which are not Special Category data but still require careful handling. Staff must take particular care when handling this information and seek advice if unsure. These include:
- 6.8.1 information relating to criminal offences or allegations;
 - 6.8.2 safeguarding information; and
 - 6.8.3 financial information where misuse could cause harm.
- 6.9 Personal Data relating to criminal convictions and offences must be handled with particular care. This type of data is subject to specific legal requirements under the Data Protection Act 2018 and must only be processed where there is a clear lawful basis and appropriate safeguards in place. Staff must not process this type of data unless authorised to do so and must seek advice from the Bursar or Head of Legal and Compliance if unsure.
- ## 7 Your Obligations
- 7.1 Personal Data must be processed lawfully, fairly and transparently at all times.
- 7.2 "Processing" includes any operation performed on Personal Data, including collection, use, storage, disclosure and deletion, including sharing (internally or externally), copying and storing it.
- 7.3 The School must provide individuals with clear information about what data is collected about them, what it is used for, and who it might be shared with. This includes information about what rights they have, how long their Personal Data is retained, and their right to complain to the Information Commissioner's Office (ICO).
- 7.4 This information must be provided when Personal Data is collected, or as soon as reasonably possible where it has not been collected directly, unless a lawful exemption applies.
- 7.5 The School provides this information through its Privacy Notices, including those relating to staff, pupils, parents (or those with parental responsibility), and where applicable, recruitment and admissions. Staff must familiarise themselves with the Privacy Notices relevant to their role.
- 7.6 Personal Data must not be used in a way which is not covered by an existing Privacy Notice or is incompatible with the purpose for which it was originally collected. Staff must consult the Bursar or Head of Legal and Compliance before proceeding.
- 7.7 You must only process Personal Data for specified, explicit and legitimate purposes, including:
- 7.7.1 ensuring that the School provides a safe and secure environment;

- 7.7.2 providing pastoral care including safeguarding, child protection and promoting the welfare of our pupils;
 - 7.7.3 in relation to HR and staff matters;
 - 7.7.4 providing education and learning for our pupils;
 - 7.7.5 providing additional activities for pupils and parents (for example extra-curricular clubs, sports or visits);
 - 7.7.6 protecting and promoting the School's interests and objectives (for example fundraising and commercial ventures); and
 - 7.7.7 to fulfil the School's contractual and other legal obligations.
- 7.8 **Use of Personal Data:** Personal Data must not be processed for purposes which are not compatible with those set out above or in the relevant Privacy Notice(s). Staff must consult the Bursar or Head of Legal and Compliance before any such processing takes place.
- 7.9 **Consent:** The School must rely on consent as a lawful basis where it is appropriate under UK data protection law. Where consent is relied upon, it must be freely given, specific, informed and unambiguous, and must be capable of being withdrawn at any time. All individuals working on behalf of the School must only process Personal Data where authorised to do so.
- 7.10 Where there is a conflict between data protection requirements and safeguarding or child protection concerns, safeguarding and the welfare of the child must take priority.
- 8 You must only process Personal Data for specified, explicit and legitimate purposes.**
- 8.1 You must not use Personal Data for purposes which are incompatible with those for which it was originally collected. Personal Data collected for one purpose must not be used for a different purpose unless this is lawful and has been communicated to the individual through an appropriate Privacy Notice. Staff must comply with all relevant School policies relating to the use of Personal Data.
- 9 Personal Data held must be adequate, relevant and limited to what is necessary for the purpose for which it is processed.**
- 9.1 Personal Data must be limited to what is necessary for the purpose for which it is processed. Staff must only collect, use or retain Personal Data where it is relevant and proportionate to the task being carried out, and must not collect, use or retain excessive or unnecessary Personal Data.
- 10 The Personal Data that you hold must be accurate.**
- 10.1 Personal Data must be accurate and kept up to date. Staff must take reasonable steps to ensure that inaccurate Personal Data is corrected without delay.
- 11 You must not keep Personal Data longer than necessary.**
- 11.1 The School's Record Keeping and Retention Policy sets out the retention periods for different categories of Personal Data and requirements for secure disposal. This applies to all Personal Data, including paper and electronic records. Staff must comply with the Record Keeping and Retention Policy and must only delete or dispose of Personal Data where authorised to do so.

- 11.2 Staff must consult the Bursar or Head of Legal and Compliance where they are uncertain about retention periods or the secure deletion of Personal Data.

12 You must keep Personal Data secure.

- 12.1 The School must implement appropriate technical and organisational measures to ensure the security of Personal Data. Personal Data must be protected at all times, whether held in paper or electronic form. This includes protecting Personal Data against unauthorised or unlawful access, disclosure, alteration or destruction, and against accidental loss or damage.
- 12.2 Staff must take appropriate steps to ensure that Personal Data is stored securely, accessed only by authorised individuals, and not disclosed improperly.
- 12.3 Staff must comply with the Information Security Policy, Acceptable Use of ICT for Staff Policy and Record Keeping and Retention Policy.

13 You must not transfer Personal Data outside the UK without adequate protection.

- 13.1 Personal Data must not be transferred outside the UK unless this has been approved by the School and appropriate safeguards are in place.
- 13.2 Staff must not transfer Personal Data outside the UK without prior approval from the Head of Legal and Compliance. This includes circumstances where Personal Data is accessed, shared or stored outside the UK, including in connection with School activities conducted overseas.
- 13.3 Where Personal Data is transferred outside the UK, the School will ensure that appropriate safeguards are in place in accordance with UK data protection law, such as adequacy regulations or approved transfer mechanisms.

14 Accountability

- 14.1 All staff are responsible for understanding and complying with their obligations under this policy in order to support the School's compliance with data protection law.
- 14.2 The School must be able to demonstrate compliance with data protection law. This includes:
- 14.2.1 maintaining records of processing activities;
 - 14.2.2 carrying out Data Protection Impact Assessments (DPIAs) where required;
 - 14.2.3 keeping records of Personal Data breaches and decisions taken; and
 - 14.2.4 ensuring appropriate training is provided to staff.

- 14.3 Personal Data must not be used in a new way, or in a way that might present a risk to individuals, without prior consultation with the Bursar or Head of Legal and Compliance.

15 Sharing Personal Data outside the School - dos and don'ts

- 15.1 The following dos and don'ts apply when sharing Personal Data outside the School:
- 15.1.1 **DO** share Personal Data on a need to know basis and only where there is a lawful basis for doing so. Think particularly carefully about why it is necessary to share

information outside of the School and if in doubt always check with the Bursar or Head of Legal and Compliance.

- 15.1.2 **DO** encrypt or password protect emails or attachments which contain Special Category Personal Data described in paragraph 6.5. For example, encryption or password protection should be used when sending details of a safeguarding or child protection incident to social services or information about pupils attending visits to visit providers or tour operators. Further information on this can be found in the Information Security policy.
- 15.1.3 **DO** obtain prior approval from the Bursar or Head of Legal and Compliance before sharing Personal Data on the School website or social media.
- 15.1.4 **DO** check with the Bursar or Head of Legal and compliance before using an app or other software that has not been authorised by the School.
- 15.1.5 **DO** share Personal Data in accordance with the School's Safeguarding (Child Protection) Policy. If you have any questions or concerns relating to safeguarding or child protection you must contact the Designated Safeguarding Lead.
- 15.1.6 **DO** be aware of "blagging" where individuals use deception to obtain Personal Data from people or organisations. Staff should seek advice from the Bursar or Head of Legal and Compliance. Do not disclose Personal Data where you are unsure of the identity or authority of the requester, including where the request appears unusual or inconsistent (for example, where a request is received from a parent using an unfamiliar or different email address). Seek advice from the Bursar or Head of Legal and Compliance if in doubt.
- 15.1.7 **DO** be aware of phishing where communications (such as emails, messages or websites) are designed to appear as if they come from a trusted source in order to obtain Personal Data or login credentials. Do not respond to suspicious communications or click on unfamiliar links, particularly where personal, financial or login information is requested. Report all concerns about phishing to the IT department immediately.
- 15.1.8 **DO NOT** disclose Personal Data to the Police without prior approval from the Head or the Bursar unless:
 - (a) there is an immediate risk to safety; or
 - (b) disclosure is required by law or necessary for the prevention or detection of crime.
- 15.1.9 **DO NOT** disclose Personal Data to contractors or service providers without prior approval from the Bursar or Head of Legal and Compliance. This includes sharing Personal Data with third parties, external providers or systems which have not been approved by the School.

16 Accessing or Sharing Personal Data within the School

- 16.1 **Sharing Personal Data:** This section applies when Personal Data is accessed or shared within the School.
- 16.2 **Need to know basis:** Personal Data must only be accessed or shared within the School on a strict "need to know" basis.

- 16.3 Examples of sharing which comply with data protection law:
- 16.3.1 a teacher discussing a pupil's academic progress with other members of staff for the purpose of supporting the pupil;
 - 16.3.2 sharing Personal Data in accordance with the School's Safeguarding (Child Protection) Policy;
 - 16.3.3 informing an exam invigilator of relevant health information necessary to support a pupil; and
 - 16.3.4 disclosing details of a pupil's allergy to bee stings to colleagues so that you/they will know how to respond where necessary to ensure the pupil's safety;
- 16.4 Examples of sharing which does not comply with data protection law:
- 16.4.1 the Head being given access to all records kept by nurses working within the School where there is no clear need to know;
 - 16.4.2 a member of staff looking at a colleague's HR records without a legitimate reason. Unauthorised access to Personal Data may constitute a disciplinary or criminal offence;
 - 16.4.3 sending full medical information about pupils to a visit provider where only limited information is necessary; and
 - 16.4.4 disclosing personal contact details for a member of staff (e.g. their home address and telephone number) to other members of staff without a lawful basis or appropriate justification.
- 16.5 **Storing Personal Data:** Personal Data must be stored in designated and secure locations in accordance with School policies.
- 16.6 **Sharing of Personal Data and safeguarding:** Personal Data may be shared where necessary to protect a pupil or other individual from harm in accordance with safeguarding and child protection obligations. All such sharing must be carried out in accordance with the School's Safeguarding (Child Protection) Policy.
- 17 Individuals' rights in their Personal Data**
- 17.1 **Rights:** Individuals have legal rights in relation to their Personal Data under UK data protection law. Staff must be able to recognise when an individual is exercising their rights and refer such requests to the Bursar. These rights can be accessed either in writing (e.g. in an email) or orally.
- 17.2 **Individual's rights:** Staff must notify the Bursar or Head of Legal and Compliance if any individual:
- 17.2.1 wants a copy of information the School holds about them or their child. This is commonly known as a subject access request;
 - 17.2.2 asks to withdraw any consent that they have given to use their information or information about their child;
 - 17.2.3 wants the School to delete any information;
 - 17.2.4 asks the School to correct or change information (unless this is a routine updating of information such as contact details);
 - 17.2.5 asks for Personal Data to be transferred back to them or to another organisation;

- 17.2.6 wants the School to stop using their information for direct marketing purposes. Direct marketing has a broad meaning for data protection purposes and might include communications such as the School newsletter or alumni events information; or
 - 17.2.7 objects to how the School is using their information or wants the School to stop using their information in a particular way, for example, if they are not happy that information has been shared with a third party.
- 17.3 Staff must not alter, block, erase, destroy or conceal information to prevent disclosure (for example to prevent its disclosure under a subject access request). Therefore, if you are asked to provide information or documents to support the School's response to a Subject Access Request, all relevant information must be provided in full and without omission.
- 17.4 **Complaints:** Individuals who have concerns about how the School handles their Personal Data should raise this in the first instance with the Bursar or Head of Legal and Compliance setting out the details of their complaint.

The School will acknowledge complaints relating to the handling of Personal Data within 30 days and will investigate and respond to such complaints without undue delay. The School will communicate the outcome of its investigation to the complainant.

Individuals also have the right to lodge a complaint with the Information Commissioner's Office (ICO) if they are not satisfied with how their Personal Data has been handled, although the ICO recommends that steps are taken to resolve the matter with the organisation before involving the regulator.

18 Requests for Personal Data (Subject Access Requests)

- 18.1 **The right to request Personal Data:** One of the most commonly exercised rights mentioned above is the right to make a Subject Access Request. Under this right, individuals are entitled to request a copy of the Personal Data which the School holds about them (or in some cases their child) and to certain supplemental information.
- 18.2 **Form of request:** Subject Access Requests do not have to be labelled as such and do not need to refer to data protection legislation to be valid. All Subject Access Requests must be referred immediately to the Bursar or Head of Legal and Compliance
- 18.3 **If a Subject Access Request is received:** Receiving a Subject Access Request is a serious matter for the School and involves complex legal rights. Staff must not respond to a subject access request unless authorised to do so. All Subject Access Requests must be handled promptly in accordance with the School's Subject Access Request Procedure.
- 18.4 **Disclosure:** When a Subject Access Request is made, the School must disclose all Personal Data within the scope of the request subject to limited exemptions under UK data protection law. There is no exemption for unprofessional or informal comments. However, this must not prevent staff from recording and sharing information where necessary to fulfil their professional duties, particularly in relation to safeguarding and child protection matters.

19 Data Breach

- 19.1 A Personal Data breach is a security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data. This includes situations where Personal Data is lost, accessed by someone who is not authorised to see it, shared in error, or altered without permission.

- 19.2 Certain Personal Data breaches must be reported to the Information Commissioner's Office (ICO) within 72 hours where they present a risk to individuals' rights and freedoms. Further information is set out in the Data Breach Policy.
- 19.3 Any breach of this policy may be treated as misconduct and may result in disciplinary action including in serious cases, dismissal.
- 19.4 **Criminal Offence:** A member of staff who deliberately or recklessly obtains or discloses Personal Data held by the School without proper authority is likely to constitute a criminal offence. It may also be a criminal offence to re-identify information which has been de-identified. For example, if names have been removed from information to protect the privacy of the individuals, those names must not be reinserted without proper authorisation from the Bursar.
- 19.5 All Personal Data breaches or suspected breaches must be reported immediately to the Bursar or Head of Legal and Compliance and escalated where necessary.
- 19.6 The School must keep a record of all Personal Data breaches, regardless of severity. See Data Breach Policy for further details.