



1.19 Data Protection Policy (EYFS & KS1-3)

Reviewer responsible:	HoF&O/Head	Date of last review:	10/26
Reviewed by:	AB/MSc	Date of next review:	10/29
Authorised by:	Exec		

Data protection policy

Introduction

1. **Introduction:** This policy sets out the School's obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025, together with relevant regulatory guidance. Data protection law regulates the way the School uses and stores information about identifiable people ("Personal Data") and provides individuals with rights in relation to that data, such as the right to access a copy of the Personal Data the School holds about them.
2. **Lawful treatment of data:** As a school, we will collect, store and process Personal Data about our staff, pupils, parents, suppliers and other third parties. We recognise that the correct and lawful treatment of this data will maintain confidence in the School and will ensure that the School operates successfully.
3. **In addition to this policy, you must also read the following which are relevant to data protection:**
 - 3.1 the School's privacy notices for staff, pupils and parents;
 - 3.2 IT acceptable use policy for staff;
 - 3.3 the information security policy; and
 - 3.4 guidance for staff on the use of photographs and videos of pupils by the School;
4. **Application:** This policy is aimed at all staff working in the School (whether directly or indirectly), whether paid or unpaid, whatever their position, role or responsibilities, which includes employees, governors, contractors, agency staff, work experience / placement students and volunteers.
5. **Obligation:** You are obliged to comply with this policy when processing Personal Data on our behalf. Any breach of this policy may result in disciplinary action.
6. **Queries:** The **Head of Finance & Operations acts as the School's Data Protection Lead**, responsible for supporting compliance with data protection law and for liaising with the Information Commissioner's Office (ICO) where necessary. All queries concerning data protection matters should be raised with the Head of Finance & Operations.

Personal Data

7. **Personal Data:** Personal Data is information that relates to a living person who can be identified either from that information alone, or from information when combined with other information. Information as simple as someone's name and address is their Personal Data.
8. **Personal Data at work:** In order for you to do your job, you will need to use and create Personal Data. Virtually anything might include Personal Data.
9. **Examples of places where Personal Data might be found are:**

- 9.1 on a computer database;
- 9.2 in a file, such as a pupil report;
- 9.3 a register or contract of employment;
- 9.4 pupils' exercise books, coursework and mark books;
- 9.5 health records; and
- 9.6 email correspondence.

10. Examples of documents where Personal Data might be found are:

- 10.1 a report about a child protection or safeguarding incident;
- 10.2 a record about disciplinary action taken against a member of staff;
- 10.3 School newsletters;
- 10.4 photographs and videos of pupils;
- 10.5 a tape recording of a job interview;
- 10.6 contact details and other personal data held about pupils, parents and staff and their families;
- 10.7 contact details of a member of the public who is enquiring about placing their child at the School;
- 10.8 financial records of a parent;
- 10.9 information on a pupil's performance; and
- 10.10 an opinion about a parent or colleague in an email.

These are just examples - there may be many other things that you use and create that would be considered Personal Data. Data Protection law requires us to be extra careful when handling personal data about children.

11. Critical School Personal Data: The following types of information are referred to as Critical School Personal Data in this policy and in the information security policy. You must be particularly careful when dealing with Critical School Personal Data.

12. Critical School Personal Data is information about:

- 12.1 safeguarding or child protection matters;
- 12.2 someone's special educational needs;
- 12.3 financial information (for example, a parent's bank details or a staff member's salary);
- 12.4 an individual's racial or ethnic origin;
- 12.5 an individual's political opinions;
- 12.6 someone's religious or philosophical beliefs;
- 12.7 trade union membership;
- 12.8 someone's physical or mental health. This includes information about the provision of health care which reveals information about their health status;
- 12.9 sex life including sexual orientation;
- 12.10 actual or alleged criminal activity;
- 12.11 serious allegations made against an individual (whether or not the allegations amount to a criminal offence and whether or not the allegations have been proved);
- 12.12 biometrics (for example fingerprints used for controlling access to a building); and
- 12.13 genetic information.
- 12.14 Special Category Data

Where the School processes special category data (Article 9 UK GDPR), such as health or safeguarding information, we do so under one or more of the following conditions:

- protecting the vital interests of the data subject;
- fulfilling employment, social security or social protection law obligations;
- provision of health or social care;
- substantial public interest (including safeguarding of children and equality of opportunity);
- explicit consent, where appropriate.

If you have any questions about your processing of these categories of Critical School Personal Data please speak to the Head of Finance & Operations.

Your obligations

13. Personal Data must be processed fairly, lawfully and transparently

13.1 What does this mean in practice?

13.1.1 "Processing" covers doing virtually anything in relation to Personal Data, including using, sharing (internally or externally), copying and storing it.

13.1.2 People must be told what data is collected about them, what it is used for, and who it might be shared with. They must also be given other information, such as, what rights they have in their data, how long we keep it for and how they may raise a data protection complaint directly with the School and about their right to ask the Information Commissioner's Office (ICO) to consider the matter after the School has had an opportunity to respond.

13.2 This information is provided in a document known as a Privacy Notice. Copies of the School's privacy notices can be obtained from the Head of Finance & Operations or accessed on the School's website. You must familiarise yourself with all of the School's privacy notices.

13.3 If you are using Personal Data in a way which someone might think is unfair please speak to the Head of Finance & Operations.

13.4 You must only process Personal Data for the following purposes:

13.4.1 ensuring that the School provides a safe and secure environment;

13.4.2 providing pastoral care including safeguarding, child protection and promoting the welfare of our pupils;

13.4.3 in relation to HR and staff matters;

13.4.4 providing education and learning for our pupils;

13.4.5 providing additional activities for pupils and parents (for example activity clubs);

13.4.6 protecting and promoting the School's interests and objectives (for example fundraising and commercial ventures); and

13.4.7 to fulfil the School's contractual and other legal obligations.

Lawful Bases for Processing

The School relies on the lawful bases set out in **Article 6 UK GDPR**, including:

- **Legal obligation** – to comply with statutory duties (e.g. safeguarding, HMRC reporting);
- **Public task** – to provide education and related activities in the public interest;
- **Legitimate interests** – to ensure the efficient operation of the School, provided these are not overridden by the rights of individuals;
- **Consent** – used rarely, and only for optional activities such as the use of pupil photographs in marketing materials.

13.5 **Use of Personal Data:** If you want to do something with Personal Data that is not on the above list, or is not set out in the relevant privacy notice(s), you must speak to the Head of Finance & Operations. This is to make sure that the School can lawfully use the Personal Data.

13.6 **Consent:** We may sometimes rely on the consent of the individual to use their Personal Data. This consent must meet certain requirements and therefore you must speak to the Head of Finance & Operations if you think that you may need to seek consent. If you are not an employee of the School (for example, if you are a volunteer), then you must be extra careful to make sure that you are only using Personal Data in a way that has been expressly authorised by the School.

14. You must only process Personal Data for specified, explicit and legitimate purposes

14.1 What does this mean in practice?

14.1.1 You must not use personal data for a reason that is incompatible with the original reason for collecting it. For example, if pupils are told that they will be photographed to enable staff to recognise them when writing references, you must not use those photographs for another purpose (e.g. in the School's prospectus). Please see the School's Code of Conduct and the guidance for staff on the use of photographs and videos of pupils by the School for further information relating to the use of photographs and videos.

15. Personal Data held must be adequate and relevant for the purpose

15.1 What does this mean in practice?

15.1.1 This means not making decisions based on incomplete data. For example, when writing reports you must make sure that you are using all of the relevant information about the pupil and when making a note of a disciplinary incident you must include all relevant details.

16. You must not collect or use excessive or unnecessary Personal Data

16.1 What does this mean in practice?

16.1.1 You must limit the Personal Data that you collect or use to the minimum needed to meet your objectives. For example, you do not need to share with all staff that a pupil has a health condition, only those staff that need to know or you must only collect information about a pupil's siblings if that Personal Data has some relevance, such as allowing the

School to determine if a sibling fee discount is applicable.

17. The Personal Data that you hold must be accurate

17.1 What does this mean in practice?

17.1.1 You must ensure that Personal Data is complete and kept up to date. For example, if a parent notifies you that their contact details have changed, you must ensure that the School's information management system has been updated.

18. You must not keep Personal Data longer than necessary

18.1 What does this mean in practice?

18.1.1 The School has a policy about how long different types of data should be kept for and when data should be destroyed. This applies to both paper and electronic documents. You must be particularly careful when you are deleting or disposing of data and must check the policy before doing so. You must only delete Personal Data if you are authorised to do so.

18.1.2 Please speak to the Head of Finance & Operations for guidance on the retention periods and secure deletion.

18.1.3 The School's retention periods are set out in the **Records Retention Policy**, which forms part of the School's data protection framework and is reviewed regularly.

19. You must keep Personal Data secure

19.1 This is a high-risk area of data protection for the School. Personal Data must be kept safe at all times. This includes paper and electronic information.

19.2 You must comply with the following School policies and guidance relating to the handling of Personal Data:

- a) [Information Security policy;]
- b) [Guidance for Staff on the use of Photographs and Videos;]
- c) IT acceptable use policy for staff; and
- d) [Information and Records Retention policy.]

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

20.1 International Transfers

Personal Data must not be transferred outside the UK without adequate safeguards. Where such transfers are necessary (for example, for an overseas school trip), the School will ensure compliance with UK GDPR by using appropriate mechanisms such as UK adequacy regulations, standard contractual clauses, or explicit consent from the individual.

21. Accountability

21.1 The School must be able to demonstrate its compliance with the data protection law. You are responsible for understanding your particular responsibilities under this policy to help ensure we meet our accountability requirements.

21.2 Before using personal data in a new way, or in a way that might present a risk to

individuals if something went wrong (e.g. before implementing new software to store medical information) please speak to the Head of Finance & Operations.

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

22. Dos and don'ts: Please review the following dos and don'ts:

- 22.1 **DO** share Personal Data on a need to know basis only - think about why it is necessary to share data outside of the School - if in doubt - always ask your Manager/the Head of Finance & Operations.
- 22.2 **DO** encrypt emails which contain Critical School Personal Data described in paragraph 11 above. For example, encryption must be used when sending details of a safeguarding or child protection incident to social services. Further information on encryption can be found in the Information Security policy.
- 22.3 **DO** make sure that you have permission from your Manager or the Head of Finance & Operations to share Personal Data on the School website or social media accounts.
- 22.4 **DO** check with your Manager or the Head of Finance & Operations before using an app or other software that has not been authorised by the School.
- 22.5 **DO** share Personal Data in accordance with the School's Safeguarding and Child Protection Policy. If you have any questions or concerns relating to safeguarding or child protection, you must contact the Designated Safeguarding Lead.
- 22.6 **DO** be aware of "blagging". This is the use of deceit to obtain Personal Data from people or organisations. You must seek advice from the Head of Finance & Operations where you are suspicious as to why the information is being requested or if you are unsure of the identity of the requester (e.g. if a request has come from a parent but using a different email address).
- 22.7 **DO** be aware of phishing. Phishing is a way of making something (such as an email or a letter) appear as if it has come from a trusted source. This is a method used by fraudsters to access valuable personal details, such as usernames and passwords. Don't reply to email, text, or pop-up messages that ask for personal or financial information or click on any links in an email from someone that you don't recognise or if you have any concerns about the message. You must report all concerns about phishing to the IT department immediately. Further information on blagging and phishing can be found in the information security policy.
- 22.8 **DO NOT** disclose Personal Data to the police without permission from the Head of Finance & Operations (unless it is an emergency).
- 22.9 **DO NOT** disclose Personal Data to contractors or service providers without permission from the Head of Finance & Operations. This includes, for example, sharing Personal Data with an external marketing team to carry out a pupil recruitment event or with an online app or website.

Accessing or sharing Personal Data within the School

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

Examples which are likely to comply with data protection law:

- 24.1 a teacher discussing a pupil's academic progress with other members of staff (for example, to ask for advice on how best to support the pupil);
- 24.2 sharing Personal Data in accordance with the School's Safeguarding and Child Protection policy;
- 24.3 informing an exam invigilator that a particular pupil suffers from panic attacks; and
- 24.4 disclosing details of a teaching assistant's allergy to bee stings to colleagues so that you / they will know how to respond (but more private health matters must be kept confidential).

Examples which are unlikely to comply with data protection law:

- 24.5 the Head being given access to all records kept by nurses working within the School (seniority does not necessarily mean a right of access);
- 24.6 a member of staff looking at a colleague's HR records without good reason. For example, if they are being nosy or suspect their colleague earns more than they do. In fact, accessing records without good reason can be a criminal offence;
- 24.7 informing all staff that a pupil has been diagnosed with dyslexia (rather than just informing those staff who teach the pupil); and
- 24.8 disclosing personal contact details for a member of staff (e.g. their home address and telephone number) to other members of staff (unless the member of staff has given permission or it is an emergency).

You must make sure that you file and save Personal Data in the correct place. For example, emails which may be needed in the future should not be stored in your inbox but instead stored somewhere centrally.

- 25. Sharing of Personal Data and safeguarding:** You may share Personal Data to avoid harm, for example in child protection and safeguarding matters. You should have received training on when to share information regarding welfare, safeguarding and child protection issues. If you have not received this training please contact the DSL as a matter of urgency.

Individuals' rights in their Personal Data

- 26. Rights:** People have various rights in their information. You must be able to recognise when someone is exercising their rights so that you can refer the matter to the Head of Finance & Operations. These rights can be exercised either in writing (e.g. in an email) or orally.
- 27. Individual's rights:** Please let the Head of Finance & Operations know if anyone (either for themselves or on behalf of another person, such as their child):
- 27.1 wants a copy of the information the School holds about them or their child. This is commonly known as a subject access request;
 - 27.2 asks to withdraw any consent that they have given to use their information or information about their child;
 - 27.3 wants the School to delete any information;
 - 27.4 asks the School to correct or change information (unless this is a routine updating of information such as contact details);

- 27.5 asks for personal data to be transferred to them or to another organisation;
 - 27.6 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
 - 27.7 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.
28. Please note, a person may be committing a criminal offence if they alter, block, erase, destroy or conceal information to prevent it from being disclosed (for example, to prevent its disclosure under a subject access request). Therefore, if you are asked to provide information or documents to a colleague who is preparing a response to a subject access request then you must make sure that you provide everything.

Requests for Personal Data (Subject Access Requests)

29. Subject Access Requests (SARs)

Individuals have the right to request a copy of the Personal Data the School holds about them (or, where appropriate, their child) and related supplementary information. Such requests can be made in any format and do not need to mention data protection specifically.

The School will normally respond within **one month** of receipt. Requests are free of charge unless manifestly unfounded, excessive or repetitive, in which case a reasonable fee may be charged or the request refused in line with UK GDPR.

All SARs must be referred immediately to the Head of Finance & Operations, who will oversee the response. Staff must not respond directly without authorisation.

Further information

- 30. **ICO website:** The School has registered its use of Personal Data with the Information Commissioner's Office and further details of the Personal Data it holds, and how it is used, can be found in the School's register entry on the Information Commissioner's website at www.ico.org.uk under registration number Z8224556. This website also contains further information about data protection.
- 31. **Contact:** If you would like any further information about anything within this policy, please contact the Head of Finance & Operations.

Breach of this policy

- 32. A breach of this policy may be treated as misconduct and could result in disciplinary action including in serious cases, dismissal.

Complaints

- 33.** Individuals have the right to complain to the School if they consider that the School has infringed their rights under data protection legislation. A data protection complaint may concern, for example, the collection, use, accuracy, disclosure, security or retention of personal data, or the School's handling of a subject access request or another data-rights request.

The School will facilitate the making of data protection complaints. Complaints may be submitted electronically, including by email, or by another appropriate means. Complaints should normally be directed to the Head of Finance & Operations, who acts as the School's Data Protection Lead. If the complaint concerns the Head of Finance & Operations, it should be directed to the Head.

The School will acknowledge receipt within 30 days; take appropriate steps to investigate and respond without undue delay, including making appropriate enquiries; keep the complainant appropriately informed; and notify the complainant of the outcome without undue delay.

The School will keep an appropriate record of the complaint, investigation, correspondence, outcome and action taken in accordance with the Document Retention Policy. Where the matter also falls within the School's general Complaints Policy, the procedures will be coordinated without restricting the individual's rights under data protection legislation. The outcome letter will explain the right to ask the ICO to consider the matter and provide appropriate contact information. No individual will be disadvantaged for raising a data protection concern or complaint in good faith.

APPENDIX 1: PRIVACY NOTICE FOR STAFF INTRODUCTION

Privacy Notice for staff

Introduction

During the course of the School's activities the School will process Personal Data about staff.

This Privacy Notice is issued under the UK GDPR and Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025. It explains how the School uses staff Personal Data, the lawful bases relied upon, the categories of data processed, how long data is retained, the rights available to staff under UK GDPR, the right to complain directly to the School, and the right subsequently to ask the ICO to consider the complaint.

This notice is aimed at all School staff and explains how the School uses Personal Data that is covered by the Data Protection Act 2018 (the Act). The School may amend this statement at any time.

The purpose of the Act is to safeguard information about individuals. The Act covers issues such as data security, an individual's rights to access their Personal Data and use and the disclosure of Personal Data.

The School is a Data Controller under the Act. This means that it is responsible for compliance with the Act.

Personal Data is information about identifiable individuals that is held on a computer or is held in a file by reference to specific criteria concerning the individual. It also applies to some other records such as certain medical records.

The Governing Body has delegated day to day responsibility for compliance with the Act to the Head of Finance & Operations. Any questions you have in relation to this policy should be directed to the Head of Finance & Operations.

What Personal Data the School holds and how it is acquired

Examples of the Personal Data which the School holds about staff include:

- information gathered during the recruitment process such as information about education and qualifications, professional achievements and suitability for the position applied for;
- information about job performance. This includes information about skills, achievements, career progression and disciplinary related matters; and
- other information about staff such as financial information, photographs, expressions of opinion or indications as to intentions regarding staff.

The School may process sensitive personal data relating to staff including:

- information about staff physical or mental health conditions in order to monitor sick leave and take decisions regarding fitness for work; and
- information about protected characteristics of staff in accordance with the School's Equal Opportunities Policy in order to monitor compliance with equal opportunities legislation.

The School may acquire Personal Data in a number of ways. For example:

- staff may provide the School with Personal Data about themselves, for example, during the recruitment process;
- Personal Data may be created internally by the School during the course of employment. An email from the Head to a member of staff complimenting them on class management would be an example of this; and
- Personal Data may be acquired from outside of the School community such as from other schools, public authorities, public sources and in connection with references

How the School uses Personal Data:

In respect of staff, the School commonly uses Personal Data for:

- ensuring that the School provides a safe and secure work environment;
- providing employment services (such as payroll and references);
- providing training and support;
- protecting and promoting our interests and objectives - this includes fundraising;
- personnel, administrative and management purposes and to enable the School to meet its legal obligations as an employer. For example, to pay staff and to monitor their performance;
- safeguarding and promoting the welfare of all staff and pupils; and
- fulfilling our contractual and other legal obligations.

The School may use Personal Data for other purposes where the Act allows and where providing an explanation would not be appropriate. For example, this includes sharing Personal Data about staff with the relevant statutory agencies investigating allegations of misconduct or for the prevention and investigation of crime and the prosecution of offenders. The School will not use Personal Data for any other purpose unless it has first communicated the other purposes or it considers it is reasonable and fair to do so.

Specific examples

CCTV: The School uses CCTV recordings for the purposes of crime prevention and investigation and also in connection with its obligation to safeguard the welfare of pupils, staff and visitors to the School site. CCTV recordings may be disclosed to third parties such as the police but only where such disclosure is in accordance with the Act. Further information about the use of CCTV can be found in the School's CCTV policy.

Photographs and video recordings: The School may use photographs and video recordings of staff for marketing and promotion purposes including in School publications, in social media and on the School website. The School may also allow external publication of media where appropriate (for example, in a local newspaper). The School may also make recordings for teaching purposes, for example, recording a drama lesson to provide feedback to pupils and staff.

Processing in line with your rights

You have the right to:

- request access to any Personal Data the School holds about you;
- ask to have inaccurate data held about you amended;

- prevent processing that is likely to cause unwarranted substantial damage or distress to you or anyone else; and
- object to any decision that significantly affects you, from being taken solely by a computer or other automated process.

Further Information

Contact: If you would like any further information about anything within this notice please contact the Head of Finance & Operations.