

Policy last reviewed	October 2025
Next Review	October 2026
Approved by SLT	October 2025
Approved by Trustees	October 2025

Data Protection, UK GDPR & Freedom of Information Policy

At St Peter & St Paul School, we aim to provide a caring environment where every child can thrive and is supported to achieve their potential. As such, we take data protection and freedom of information seriously.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the trust complies with the following core principles of the GDPR.

1. Aims

St Peter & St Pauls School aims to ensure that all data collected about staff, pupils, parents and visitors is collected, stored and processed in accordance with the Data Protection Act 2018 and UK GDPR regulations.

This policy applies to all data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the [Data Protection Act 2018](#), and is based on [guidance published by the Information Commissioner's Office](#) and [model privacy notices published by the Department for Education](#).

It also takes into account the expected provisions of the [General Data Protection Regulation 2018](#).

In addition, this policy complies with regulation 5 of the [Education \(Pupil Information\) \(England\) Regulations 2005](#), which gives parents the right of access to their child's educational record.

This policy complies with our funding agreement and articles of association.

3. Definitions

Term	Definition
Personal data	Data from which a person can be identified, including data that, when combined with other readily



	available information, leads to a person being identified
Sensitive personal data	Data such as: <ul style="list-style-type: none">• Contact details• Racial or ethnic origin• Political opinions• Religious beliefs, or beliefs of a similar nature• Where a person is a member of a trade union• Physical and mental health• Sexual orientation• Whether a person has committed, or is alleged to have committed, an offence• Criminal convictions
Processing	Obtaining, recording or holding data
Data subject	The person whose personal data is held or processed
Data controller	A person or organisation that determines the purposes for which, and the manner in which, personal data is processed
Data processor	A person, other than an employee of the data controller, who processes the data on behalf of the data controller

4. The data controller

Our school processes personal information relating to pupils, staff and visitors, and, therefore, is a data controller. Our school delegates the responsibility of data controller to the Bursar.

The school is registered as a data controller with the Information Commissioner's Office and renews this registration annually.

5. Data protection principles

The Data Protection Act 2018 is based on the following data protection principles, or rules for good data handling:

- Data shall be processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful purposes
- Personal data shall be relevant and not excessive in relation to the purpose(s) for which it is processed
- Personal data shall be accurate and, where necessary, kept up to date
- Personal data shall not be kept for longer than is necessary for the purpose(s) for which it is processed
- Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 2018 and UK GDPR legislation.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless the country or territory ensures an adequate level of protection for the rights and freedoms of data in relation to the processing of personal data.

6. Roles and responsibilities

The Board of Trustees has overall responsibility for ensuring that the school complies with its obligations under the Data Protection Act 2018 and UK GDPR.

Day-to-day responsibilities rest with the Headteacher and Bursar. The Headteacher and Bursar will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.

Staff are responsible for ensuring that they collect and store any personal data in accordance with this policy. Staff must also inform the school of any changes to their personal data, such as a change of address.

7. Privacy/fair processing notice

7.1 Pupils and parents

We hold personal data about pupils to support teaching and learning, to provide pastoral care and to assess how the school is performing. We may also receive data about pupils from other organisations including, but not limited to, other schools, local authorities and the Department for Education. This data includes, but is not restricted to:

- Contact details
- Results of internal assessment and externally set tests
- Data on pupil characteristics, such as ethnic group or special educational needs
- Exclusion information

- Details of any medical conditions.

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about pupils with anyone without consent unless the law and our policies allow us to do so. Individuals who wish to receive a copy of the information that we hold about them/their child should refer to sections 8 and 9 of this policy.

We are required, by law, to pass certain information about pupils to specified external bodies, such as our local authority and the Department for Education, so that they are able to meet their statutory obligations.

7.2 Staff

We process data relating to those we employ to work at, or otherwise engage to work at, our school. The purpose of processing this data is to assist in the running of the school, including to:

- Enable individuals to be paid
- Facilitate safe recruitment
- Support the effective performance management of staff
- Improve the management of workforce data across the sector
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Support the work of the School Teachers' Review Body

Staff personal data includes, but is not limited to, information such as:

- Contact details
- National Insurance numbers
- Salary information
- Qualifications
- Absence data
- Personal characteristics, including ethnic groups
- Medical information
- Outcomes of any disciplinary procedures.

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about staff with third parties without consent unless the law allows us to.

We are required, by law, to pass certain information about staff to specified external bodies, such as our local authority and the Department for Education, so that they are able to meet their statutory obligations.

Any staff member wishing to see a copy of information about them that the school holds should contact the Headteacher.

8. Subject access requests

Under the Data Protection Act 2018 and UK GDPR, pupils have a right to request access to information the school holds about them. This is known as a Subject Access Request.

Subject Access Requests must be submitted in writing, either by letter, email or fax and will be completed within one month of the date received. For complex requests this can be extended by a further two months. Requests should include:

- The pupil's name
- A correspondence address
- A contact number and email address
- Details about the information requested

The school will not reveal the following information in response to subject access requests:

- Information that might cause serious harm to the physical or mental health of the pupil or another individual
- Information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests
- Information contained in adoption and parental order records
- Certain information given to a court in proceedings concerning the child.

9. Parental requests to see the educational record

Parents have the right of access to their child's educational record, free of charge, within 15 school days of a request.

Personal data about a child belongs to that child, and not the child's parents. This is the case even where a child is too young to understand the implications of subject access rights.

For a parent to make a subject access request, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

10. Storage of records

- Paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal information are kept secured when not in use
- Papers containing confidential personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access
- Where personal information needs to be taken off site (in paper or electronic form), staff must sign it in and out from the school office and will be encrypted where applicable.
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or trustees who store personal information belonging to other's on their personal devices must follow the same security procedures for school-owned equipment and must sign the agreement applicable to this.

11. Disposal of records

Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely.

For example, we will shred or incinerate paper-based records, and override electronic files. We may also use an outside company to safely dispose of electronic records.

12. Data breaches

- The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- The Headteacher will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.
- Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed as well as the effected party/parties.



- All notifiable breaches will be reported to the relevant supervisory authority and effected party/parties within 72 hours of becoming aware of it.

13. Training

Our staff and trustees are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation or the school's processes make it necessary.

14. The General Data Protection Regulation

We acknowledge that the General Data Protection Regulation came into force in May 2018.

We reviewed working practices when this new legislation took effect.

15. Monitoring arrangements

The Bursar is responsible for monitoring and reviewing this policy.

The Bursar checks that the school complies with this policy by, among other things, reviewing school records on a regular basis.

This document will be reviewed **annually**.

At every review, the policy will be shared with the Board of Trustees.

Bursar

October 2025

Note: A review of this policy, through the Trustee Board and the SLT, is undertaken within 1 year of the last review date.