St Peter &
St Paul School

Policy last reviewed	28/10/2026
Next Review	28/10/2027
Approved by SLT	October 2026
Approved by Trustees	October 2026

Data protection Policy

1. Purpose and scope

St Peter & St Paul School is committed to handling personal data lawfully, fairly and securely. This policy sets out how the School protects personal data and what is expected of anyone handling it on the School's behalf.

The policy applies to staff, trustees, volunteers and others who handle personal data for the School. It covers information about pupils, prospective pupils, parents and carers, staff, job applicants, trustees, volunteers, visitors and other individuals. It applies to information in any format, including paper records, emails, photographs, video and information held in systems operated by the School or by suppliers on its behalf.

2. Legislation and data protection principles

The School handles personal data in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025. The School also complies with the Privacy and Electronic Communications Regulations where they apply, including to relevant electronic marketing and the use of cookies and similar technologies.

The School will ensure that personal data is:

- Processed lawfully, fairly and transparently.
- Collected for specified, explicit and legitimate purposes and used in ways compatible with those purposes.
- Adequate, relevant and limited to what is necessary.
- Accurate and kept up to date where necessary.
- Kept in identifiable form only for as long as necessary.
- Protected against unauthorised or unlawful processing and accidental loss, destruction or damage.

The School is responsible for demonstrating compliance with these principles.

3. Definitions

Term	Meaning
Personal data	Information relating to a living person who can be identified directly or indirectly. Examples include names, contact details, pupil records and identifiable photographs.
Special category data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. It also includes genetic data, biometric data used to identify a person uniquely, health data, and data about a person's sex life or sexual orientation.
Criminal offence data	Personal data about criminal convictions, offences, allegations, proceedings or related security measures. It can include information disclosed through a DBS check.
Processing	Anything done with personal data, including collecting, recording, storing, accessing, updating, sharing, deleting or destroying it.
Data subject	The person the personal data relates to.
Data controller	The person or organisation that determines why and how personal data is processed.
Data processor	A person or organisation that processes personal data on behalf of the controller, such as a supplier that hosts records on the School's instructions.
Personal data breach	A security incident that results in the accidental or unlawful destruction, loss or alteration of personal data, or unauthorised disclosure of or access to it.

4. Roles and responsibilities

The School as data controller
[Insert full registered legal name], operating as St Peter & St Paul School, is the data controller. The School determines why and how it uses personal data and is accountable for compliance with data protection law.

Board of Trustees
The Board oversees compliance, approves this policy and receives reports on significant data protection risks or incidents as appropriate.

Headteacher
The Headteacher supports implementation of this policy and ensures staff understand

their responsibilities. Where a data protection matter raises a safeguarding concern, the Headteacher and School Business & Development Manager will work with the Designated Safeguarding Lead in line with the School's safeguarding procedures.

School Business & Development Manager
The School delegates day-to-day responsibility for data protection to the School Business & Development Manager, who acts as the School's designated data protection lead. The Manager advises staff, maintains relevant records and procedures, coordinates responses to requests and complaints, and manages personal data breaches and any required notifications on the School's behalf. The Manager also checks the School's ICO data protection fee requirements annually and arranges renewal where required.

Staff, trustees and volunteers
Anyone handling personal data on the School's behalf must follow this policy, use approved systems, access only the information needed for their role and promptly report requests, concerns and suspected breaches. Staff must tell the School when their own personal details change so that records can be kept up to date.

5. Using personal data and providing privacy information

The School identifies and records an appropriate lawful basis for processing personal data. Where it processes special category data or criminal offence data, it also identifies the applicable legal condition and applies any required safeguards.

The School uses pupil and family information for purposes including admissions, teaching and assessment, pastoral care, safeguarding, attendance, medical support and communication with parents and carers. This may include information received from families, previous schools, local authorities and other relevant organisations.

The School uses staff and applicant information for purposes including safer recruitment, employment administration, payroll, absence management, training, performance management and workforce planning.

The School's privacy notices explain what personal data it collects, where it comes from, why it is used, the applicable lawful bases, who may receive it, how long it is kept or how retention is decided, and how individuals can exercise their rights. Information about the School's use of website cookies and similar technologies is provided through its website privacy and cookie information.

6. Sharing personal data and using suppliers

The School shares personal data where it has a lawful basis and the sharing is necessary for the purpose. Staff must check the recipient's identity and authority where appropriate, share only the information needed and use a secure method. The School will provide information to public bodies where a legal obligation applies.

Where a concern relates to a child's safety or welfare, staff must follow the School's safeguarding procedures and share information promptly where necessary and lawful to protect the child.

Where a supplier processes personal data on the School's behalf, the School checks that the supplier provides appropriate safeguards and puts the required contractual terms in place. The School assesses any proposed restricted international transfer and ensures that it meets the applicable UK data protection requirements before proceeding.

7. Individual rights and subject access requests

Depending on the circumstances, individuals may have the right to access or correct their personal data, request erasure or restriction, object to processing, receive certain data in a portable format, or exercise safeguards in relation to automated decisions. Where the School relies on consent, individuals can withdraw it.

A subject access request can be made verbally or in writing to any member of staff. Staff must record the date it was received and pass it promptly to the School Business & Development Manager. The School will verify the requester's identity or authority to act where necessary.

The School will respond without undue delay and normally within one month. Where a lawful extension applies, the School will notify the requester within the initial one-month period and explain the reason. The same statutory timescales apply during school holidays.

A pupil who can understand the right of access and what making a request means can exercise that right themselves. A parent or carer may act on the pupil's behalf if the pupil authorises them, or if the pupil cannot exercise the right independently and the School is satisfied that the person can properly act on their behalf. The School will consider the pupil's interests and confidentiality, safeguarding concerns, the rights of other people and any applicable exemptions before disclosing information.

8. Storage, portable devices and information security

Paper records and workspaces
Keep confidential paper records in secure storage when they are not in use. Do not leave them on desks, in classrooms or in shared areas where unauthorised people could see or access them. Lock screens when leaving a device unattended.

Portable devices and removable media
Laptops, tablets, phones, external drives and USB devices used to store School personal data must be approved for that use and encrypted. Keep them secure when not in use and during transport. Report any loss or theft immediately under the School's data breach procedure.

Personal devices
Staff, trustees and pupils may use personal devices to handle other people's personal data on behalf of the School only with prior authorisation and after signing the applicable device-use agreement. They must follow the School's security requirements for that use.

Accounts and passwords
Use approved School accounts and systems. Keep passwords confidential, use a unique password for each account and follow the School's IT requirements for passwords and multi-factor authentication. Report suspected account compromise immediately and change affected passwords promptly.

9. Retention and secure disposal

The School keeps personal data in line with its retention arrangements and corrects inaccurate information where necessary. Records needed for safeguarding, an investigation, a legal claim or another continuing obligation will be preserved for as long as required.

When records are due for disposal, confidential paper records must be shredded or collected by an approved confidential waste service. Electronic records and storage media must be securely erased or destroyed. Where an external provider is used, the School will check that it can dispose of the information securely.

10. Personal data breaches

Anyone handling School personal data must report an actual or suspected breach immediately to the School Business & Development Manager. If the Manager is unavailable, report it to the Headteacher. Examples include sending information to the wrong recipient, losing records or a device, and discovering unauthorised access to an account.

The School will take steps to contain the breach, assess the risk to individuals and record the incident, the decisions made and the action taken. The School will record all personal data breaches, including those that do not require external notification.

The School will notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of a breach, unless the breach is unlikely to result in a risk to individuals' rights and freedoms. Where a breach is likely to result in a high risk to individuals, the School will inform those affected without undue delay, subject to any applicable legal exception.

11. Data protection complaints

Anyone concerned about how the School handles their personal data can raise a complaint with the School Business & Development Manager using the contact details at the top of this policy.

The School will acknowledge the complaint within 30 days of receipt, take appropriate steps to investigate it and communicate the outcome without undue delay. Individuals can also raise a concern with the ICO. The School's privacy notices provide details of how to contact the ICO.

12. Training, monitoring and review

The School provides data protection training to staff and trustees at induction, with refresher training as appropriate. Training covers how to handle personal data securely, recognise requests and identify and report breaches.

The School Business & Development Manager monitors compliance, reviews relevant records and procedures, and coordinates data protection impact assessments where proposed processing is likely to result in a high risk to individuals.

The School Business & Development Manager reviews this policy annually and following significant changes to legislation or School practice. The Senior Leadership Team reviews the policy before it goes to the Board of Trustees for approval.