SS Peter & Paul
CATHOLIC PRIMARY SCHOOL

Data Protection Policy

Approved by	**Full Governing Body**
Date approved	**3 September 2025**
Last reviewed on	**October 2026**
Next review due by	**September 2027**
Policy lead	**Headteacher, advised by the Data Protection Officer**
Version	**2.0 (supersedes version 1.0, September 2025)**

'Learning Together, Achieving Together in Christ'

Version control

Version	Date	Summary of changes	Approved
1.0	September 2025	Data protection policy based on the UK GDPR and Data Protection Act 2018.	FGB
2.0	October 2026	Moved to the school policy template. Updated for the Data (Use and Access) Act 2025, including the new right to complain to the school (in force 19 June 2026), reasonable and proportionate searches for subject access requests, and the change from the Information Commissioner's Office to the Information Commission (30 September 2026). Removed EU-only text that does not apply in the UK. Added the parental right of access to the educational record, criminal offence data, artificial intelligence, training, and roles. DPO details flagged for confirmation.	FGB

Contents

1. Introduction and Statement of Intent
2. Scope
3. Legal and Statutory Framework
4. Definitions
5. Roles and Responsibilities
6. Data Protection Principles
7. Accountability
8. Lawful Processing
9. Consent
10. The Right to Be Informed
11. The Right of Access
12. Other Individual Rights
13. Data Protection Complaints
14. Data Protection by Design and Impact Assessments
15. Personal Data Breaches
16. Data Security
17. Educational Visits
18. Safeguarding and Information Sharing
19. Publication of Information
20. CCTV and Photography
21. Data Retention and Disposal
22. DBS Data
23. Artificial Intelligence
24. Training
25. Monitoring and Review

1. Introduction and Statement of Intent

SS Peter & Paul Catholic Primary School is committed to being transparent about how it collects and uses personal data, and to meeting its data protection obligations. We hold information about pupils, families, staff, governors, volunteers and others because we need it to educate and care for children and to run the school. People trust us with that information, and we treat that trust seriously.

This policy explains how the school complies with data protection law and sets out the responsibilities of everyone who handles personal data on the school's behalf. It should be read with the school's privacy notices and with the HR policies that cover the personal data of job applicants, employees, workers, contractors, volunteers and former employees.

The school may need to share personal information with other organisations, including the local authority, the Department for Education, other schools, the Archdiocese of Southwark, social care services and the police. Any sharing is lawful, proportionate and in line with this policy.

2. Scope

This policy applies to all personal data processed by the school, in any format, including paper records, electronic records, email, images, video and audio recordings, and data held in third-party systems used by the school.

It applies to all staff, governors, volunteers, contractors and anyone else who processes personal data on the school's behalf, wherever that processing takes place, including at home and on personal devices.

3. Legal and Statutory Framework

This policy has due regard to all relevant legislation and guidance, including but not limited to:

Legislation

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Data (Use and Access) Act 2025
- Freedom of Information Act 2000
- Privacy and Electronic Communications Regulations 2003
- Education (Pupil Information) (England) Regulations 2005, as amended
- Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- School Standards and Framework Act 1998

Guidance

- Information Commission (formerly the Information Commissioner's Office), guidance on the UK GDPR, subject access, complaints handling, and the Age appropriate design code
- DfE, Data protection in schools
- DfE, Keeping Children Safe in Education 2026

- HM Government, Information sharing: advice for practitioners providing safeguarding services
- Information and Records Management Society, Records Management Toolkit for Schools

This policy is implemented alongside the following school policies:

- Online Safety and Acceptable Use of Smart Devices Policy
- Safe Use of Artificial Intelligence (AI) Policy
- Safeguarding and Child Protection Policy
- Freedom of Information Policy and Publication Scheme
- Retention Policy
- Cyber Security Policy

4. Definitions

- **Personal data:** any information relating to an identified or identifiable living individual (a "data subject"). A person is identifiable if they can be identified directly or indirectly, for example by name, an identification number, location data, an online identifier, or factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity.
- **Special category data:** personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; genetic data; biometric data used to identify a person; data concerning health; and data concerning a person's sex life or sexual orientation.
- **Criminal offence data:** personal data relating to criminal convictions and offences or related security measures, including information from Disclosure and Barring Service (DBS) checks.
- **Processing:** anything done with personal data, including collecting, recording, organising, storing, adapting, retrieving, using, disclosing, sharing, restricting, erasing or destroying it, whether or not by automated means.
- **Data controller:** the organisation that decides why and how personal data is processed. For SS Peter & Paul, the controller is the Governing Body.
- **Data processor:** an organisation that processes personal data on the controller's behalf, such as a software or IT provider.
- **Personal data breach:** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- **Consent:** any freely given, specific, informed and unambiguous indication of a person's wishes, by a statement or clear affirmative action, agreeing to the processing of their personal data.
- **Filing system:** any structured set of personal data that is accessible according to specific criteria.
- **Data Protection Officer (DPO):** the person who informs and advises the school about its data protection obligations and monitors compliance.

5. Roles and Responsibilities

The Governing Body

As the data controller, the Governing Body has overall responsibility for making sure the school complies with data protection law, and receives an annual report on data protection from the Headteacher.

The Headteacher

Responsible for day-to-day compliance, for making sure staff are trained and aware of their responsibilities, and for acting on the DPO's advice. The Headteacher is the senior lead for data protection. SchoolPro, as the school's data protection platform, supports the Headteacher and the DPO.

The Data Protection Officer

The school has appointed a Data Protection Officer as required for public authorities. The DPO service is provided by School Pro Ltd.

The DPO:

- informs and advises the school and its staff about their data protection obligations;
- monitors compliance, including through audits and reviewing records of processing;
- advises on Data Protection Impact Assessments (DPIAs);
- advises on whether a breach must be reported to the Information Commission or to the people affected;
- is the point of contact for the Information Commission and for data subjects.

The DPO reports to the highest level of management, operates independently, is given the resources needed to carry out the role, and is not dismissed or penalised for performing it. The DPO works with the Designated Safeguarding Lead so that pupil data is protected while information that keeps children safe is shared appropriately.

Suspected breaches and incidents are reported through the DPO's reporting route **via School Pro platform.**

All staff

All staff process personal data in line with this policy, complete data protection training, report any suspected breach immediately, and seek advice from the data protection lead or DPO when unsure.

6. Data Protection Principles

Personal data will be:

1. processed lawfully, fairly and in a transparent manner;
2. collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes (further processing for archiving in the public interest, research or statistical purposes is not regarded as incompatible);
3. adequate, relevant and limited to what is necessary;
4. accurate and, where necessary, kept up to date, with every reasonable step taken to erase or correct inaccurate data without delay;

5. kept in a form that permits identification of individuals for no longer than is necessary;
6. processed securely, with protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

The school is responsible for, and must be able to demonstrate, compliance with these principles (the accountability principle).

7. Accountability

The school implements appropriate technical and organisational measures to demonstrate that data is processed in line with the principles, and provides clear and transparent privacy notices.

The school keeps a record of processing activities, which includes:

- the name and contact details of the school and the DPO;
- the purposes of processing;
- the categories of individuals and of personal data;
- the categories of recipients;
- details of any transfers outside the UK and the safeguards in place;
- retention periods;
- a description of the technical and organisational security measures.

The school applies data protection by design and by default, including data minimisation, pseudonymisation where practical, transparency, and the continuous improvement of security.

8. Lawful Processing

8.1 Personal data

The lawful basis for processing is identified and documented before processing begins. Under Article 6 of the UK GDPR, data is processed lawfully where at least one of the following applies:

1. the data subject has given consent;
2. processing is necessary for a contract with the data subject;
3. processing is necessary to comply with a legal obligation;
4. processing is necessary to protect someone's vital interests;
5. processing is necessary for a task carried out in the public interest or in the exercise of official authority;
6. processing is necessary for legitimate interests, or for a recognised legitimate interest under the Data (Use and Access) Act 2025, except where those interests are overridden by the rights of the data subject.

As a public authority, the school relies mainly on public task and legal obligation. Legitimate interests cannot be relied on for processing carried out in the performance of the school's public tasks. The DPO advises where the correct basis is unclear.

8.2 Special category data

To process special category data, the school identifies both an Article 6 basis and a separate condition under Article 9 of the UK GDPR, supported where required by a condition in Schedule 1 of the Data Protection Act 2018. The conditions the school most commonly relies on are:

- the explicit consent of the data subject;
- obligations in employment, social security and social protection law;
- protecting the vital interests of a person who cannot give consent;
- the establishment, exercise or defence of legal claims;
- reasons of substantial public interest, including statutory and government purposes, equality of opportunity, and safeguarding of children and individuals at risk;
- preventive or occupational medicine and the provision of health or social care;
- public health;
- archiving, research and statistical purposes.

The school keeps an appropriate policy document where Schedule 1 of the Data Protection Act 2018 requires one.

8.3 Criminal offence data

Criminal offence data, including DBS information, is processed only where authorised by law, under a condition in Schedule 1 of the Data Protection Act 2018, and in line with section 21 of this policy.

9. Consent

Where consent is the lawful basis, it must be a positive indication of agreement. It cannot be inferred from silence, inactivity or pre-ticked boxes. Consent is only accepted where it is freely given, specific, informed and unambiguous, and a record is kept of how and when it was given.

Consent can be withdrawn at any time, and it must be as easy to withdraw as to give. Where consent cannot meet these standards, another lawful basis is found or the processing stops.

For pupils, consent is normally sought from a parent or carer. In the UK, a child aged 13 or over may give their own consent to online (information society) services offered directly to them. Pupils at SS Peter & Paul are under 13.

10. The Right to Be Informed

The school publishes privacy notices for pupils and parents, staff, governors, volunteers and job applicants. Privacy notices are written in clear, plain language, are concise, transparent and easily accessible, and are free of charge. Where a service is offered directly to a child, the notice is written so the child can understand it.

Privacy notices set out:

1. the identity and contact details of the school and of the DPO;
2. the purposes of processing and the lawful basis;
3. any legitimate interests relied on;

4. the recipients or categories of recipients;
5. any transfers outside the UK and the safeguards in place;
6. how long data will be kept, or the criteria used to decide this;
7. the rights of access, rectification, erasure, restriction, objection and portability;
8. the right to withdraw consent, where consent is the basis;
9. the right to complain to the school and then to the Information Commission;
10. whether providing the data is a statutory or contractual requirement, and the consequences of not providing it;
11. the existence of any automated decision-making, including meaningful information about the logic involved and its consequences.

11. The Right of Access

11.1 Subject access requests

Individuals have the right to confirm whether their data is being processed and to receive a copy of it. A subject access request (SAR) can be made verbally or in writing to any member of staff, who passes it to the data protection lead immediately.

- The school verifies the identity of the requester before releasing information.
- Information is provided free of charge. A reasonable fee may be charged for further copies, or where a request is manifestly unfounded or excessive, based on administrative cost.
- The school responds without undue delay and at the latest within one month of receipt.
- The time limit may be extended by up to two further months where requests are complex or numerous. The requester is told of the extension, and why, within the first month.
- Where the school needs to confirm the requester's identity or reasonably needs clarification of the request, the time limit is paused until that information is received, as provided for by the Data (Use and Access) Act 2025.
- The school carries out reasonable and proportionate searches for the information requested.
- Where a request is made electronically, information is provided in a commonly used electronic format unless the requester asks otherwise.
- Where a request is manifestly unfounded or excessive, the school may refuse it. The requester is told the reasons and their right to complain to the Information Commission and to seek a judicial remedy.

Information about other people, and information that falls under an exemption (for example, where disclosure would be likely to cause serious harm to a child), is withheld or redacted in line with the law and DPO advice.

11.2 Requests from or about children

Personal data about a child belongs to the child, even when a parent makes the request. For pupils of primary age, requests from parents are usually granted, but the school considers the child's best interests and whether the child is mature enough to understand their rights.

11.3 Parental access to the educational record

Separately from the right of subject access, parents of pupils at a maintained school have a right under the Education (Pupil Information) (England) Regulations 2005 to see their child's educational record free of charge within 15 school days of a written request, and to receive a copy for a fee that does not exceed the cost of supply.

12. Other Individual Rights

12.1 Rectification

Individuals are entitled to have inaccurate or incomplete personal data corrected. Where the data has been disclosed to third parties, the school informs them of the rectification where possible, and tells the individual who those third parties are where appropriate. Requests are answered within one month, extendable by two months where complex. Where no action is taken, the school explains why and tells the individual of their right to complain.

12.2 Erasure

Individuals may ask for their data to be deleted where there is no compelling reason for its continued processing, including where:

- the data is no longer necessary for the purpose it was collected for;
- the individual withdraws consent and there is no other lawful basis;
- the individual objects and there is no overriding legitimate ground;
- the data was processed unlawfully;
- erasure is needed to comply with a legal obligation;
- the data was collected in relation to an online service offered to a child.

The school may refuse erasure where processing is necessary to exercise freedom of expression and information, to comply with a legal obligation or perform a public task, for public health, for archiving, research or statistics, or for legal claims. Particular weight is given to requests to erase data originally provided when the individual was a child. Where data has been shared, recipients are informed unless this is impossible or involves disproportionate effort.

12.3 Restriction of processing

Individuals may ask the school to restrict processing where they contest the accuracy of the data, where processing is unlawful but they do not want the data erased, where the school no longer needs the data but they need it for a legal claim, or while an objection is being considered. Restricted data is stored but not otherwise used, and individuals are told before a restriction is lifted.

12.4 Data portability

The right to data portability applies only to personal data an individual has provided to the school, where processing is based on consent or a contract and is carried out by automated means. Most school processing is carried out as a public task, so the right rarely applies. Where it does, data is provided in a structured, commonly used and machine-readable format within one month and free of charge.

Pupil records are transferred to other schools securely through School to School (S2S), the DfE's secure data transfer service, and through the school's management information system.

12.5 The right to object

Individuals are told of their right to object in the school's privacy notices. They may object to processing based on public task or legitimate interests on grounds relating to their particular situation, and the school stops processing unless it can show compelling legitimate grounds, or the processing is needed for legal claims. Objections to direct marketing are always upheld. Where an objection is refused, the school explains why within one month and tells the individual of their right to complain.

12.6 Automated decision-making

The school does not make significant decisions about individuals by solely automated means. Decisions about pupils, including those relating to attainment, SEND provision, behaviour, attendance, admissions and safeguarding, always involve meaningful human judgement. This is set out further in the Safe Use of Artificial Intelligence (AI) Policy.

13. Data Protection Complaints

Under the Data (Use and Access) Act 2025, from 19 June 2026 anyone may complain to the school about the way it has handled their personal data. The school:

- makes it easy to complain, including by email, in writing or by using a complaint form;
- acknowledges a complaint within 30 days of receiving it;
- takes appropriate steps to respond without undue delay, including making enquiries and keeping the complainant informed;
- tells the complainant the outcome.

Data protection complaints are handled by the data protection lead with advice from the DPO, separately from the general Complaints Procedure. If a complainant is not satisfied with the school's response, they may complain to the Information Commission (ico.org.uk).

14. Data Protection by Design and Impact Assessments

The school builds data protection into new processing from the start. A Data Protection Impact Assessment (DPIA) is completed, with the DPO's advice, before any processing that is likely to result in a high risk to individuals, including:

- introducing new technology or systems that process personal data, including AI tools;
- large-scale processing of special category or criminal offence data;
- systematic monitoring, such as CCTV or online monitoring;
- profiling or automated decision-making.

Each DPIA describes the processing and its purposes, assesses necessity and proportionality, identifies risks to individuals, and sets out the measures to address them. Where a DPIA shows a high risk that cannot be reduced, the school consults the Information Commission before processing begins.

15. Personal Data Breaches

A personal data breach may be:

- a confidentiality breach: unauthorised or accidental disclosure of, or access to, personal data;
- an availability breach: accidental or unauthorised loss of access to, or destruction of, personal data;
- an integrity breach: unauthorised or accidental alteration of personal data.

Any member of staff who suspects a breach reports it immediately to the data protection lead or Headteacher, who reports it to the DPO without delay.

- Every breach is recorded, whether or not it is reported externally, including the facts, its effects and the action taken.
- Where a breach is likely to result in a risk to people's rights and freedoms, it is reported to the Information Commission within 72 hours of the school becoming aware of it.
- Where a breach is likely to result in a high risk to people's rights and freedoms, the people affected are told without undue delay.
- A breach notification sets out the nature of the breach, including the categories and approximate number of people and records concerned; the DPO's contact details; the likely consequences; and the measures taken or proposed to deal with it and to reduce any adverse effects.

The school identifies the cause of each breach and how to prevent a recurrence, for example through refresher training where human error was involved. Failure to report a notifiable breach may lead to enforcement action. Unauthorised disclosure by staff may lead to disciplinary action.

16. Data Security

16.1 Paper records

- Confidential paper records are kept in a locked filing cabinet, drawer or safe with restricted access, and are not left unattended or in view in areas with general access.
- The School Business Manager, the Designated Safeguarding Leads and the SENCO have lockable security pouches for sensitive documents that need to be taken off site.
- Visitors to areas containing sensitive information are supervised at all times.

16.2 Electronic records and devices

- Digital data is protected through appropriate security measures, including encryption and password protection, where applicable. School data is backed up securely off site to support data recovery in the event of data loss, system failure or a cyber incident. The school's backup arrangements and security measures are maintained in consultation with the IT provider.
- Removable storage and portable devices that hold personal data are encrypted to AES-256 standard and stored securely when not in use. Memory sticks are not used for personal data unless they are encrypted.
- All devices are password-protected, and where possible can be locked or wiped remotely if lost or stolen.
- Staff have their own secure login. Multi-factor authentication is used for school email, cloud services and remote access.

- Staff and governors save school documents only to the school's approved cloud storage, never to the hard drive of a personal device, and never use personal email or personal cloud storage for school business.
- Remote access to the school network is granted on a business need and uses multi-factor authentication.
- Wi-Fi on the school network is for school devices. Staff-owned devices and visitors use the separate guest network.
- Access to files is on a need-to-know basis, with permissions set by role, and access is monitored and reviewed.

16.3 Email and transfers

- Email is not a secure way to send sensitive information externally and is used only as a last resort. Sensitive documents sent by email are encrypted or password-protected, with the password sent separately.
- The school uses secure transfer services, including S2S, for sending personal data to other organisations.
- Group emails to parents are sent using blind copy (bcc) or the school's communication system, so that addresses are not shared.

16.4 Taking data off site

Staff who take personal data off site, on paper or electronically, keep it secure at all times, for example under lock and key, and accept responsibility for its security.

Before sharing data, staff make sure that they are allowed to share it, that adequate security is in place, and that the recipient is covered by a privacy notice.

16.5 Physical security and continuity

The physical security of buildings and storage is reviewed termly, and extra measures are put in place if the risk of break-in or theft increases. The school maintains continuity and recovery arrangements for its systems, with advice from the DPO and IT provider.

17. Educational Visits

Where personal data is taken on an educational visit, staff make sure that:

- risk assessments and other sensitive documents are managed securely on the day;
- documents are kept in staff members' bags when not being referred to;
- different documents (for example risk assessments, tickets, maps and groupings) are kept in separate wallets to limit the impact if one is lost;
- information given to parent helpers or other adults is on a need-to-know basis only, for example the medical needs of the children in their group;
- all documents given to other adults are collected back by the visit leader at the end of the visit.

18. Safeguarding and Information Sharing

Data protection law does not prevent or limit the sharing of information for the purposes of keeping children safe. The Data Protection Act 2018 includes "safeguarding of children and individuals at risk" as a condition that allows information, including special category data, to be shared without consent where consent cannot be obtained, cannot reasonably be expected, or would place a child at risk.

The school shares information relevant to identifying, assessing and responding to risks to a child with the right people and agencies, proactively and as soon as reasonably possible. Where there is doubt about sharing, the DSL records:

- whether information was shared, what was shared, with whom, and why;
- where a decision was made not to seek consent, and the reason.

The school seeks consent to share information where appropriate, but does not seek it where doing so would place a child at risk.

19. Publication of Information

The school publishes a publication scheme on its website setting out the classes of information it makes routinely available, including policies and procedures, annual reports and financial information. These are available on the website or quickly on request.

The school does not publish personal information, including photographs, on its website without the permission of the person concerned or, for pupils, a parent. Staff check documents and images for hidden metadata, tracked changes and other identifying details before uploading them.

20. CCTV and Photography

20.1 CCTV

The school uses CCTV for the safety and security of the site. Recording images of identifiable people is processing personal data, and the school operates CCTV in line with the data protection principles and Information Commission guidance.

- Signs tell pupils, staff and visitors that CCTV is in operation and why.
- Cameras are placed only where needed and never in private areas such as toilets or changing areas.
- Footage is kept for no longer than necessary and is automatically overwritten after 30 days unless it is needed for an investigation.The Headteacher is responsible for the CCTV system and for authorising access to footage. The DPO advises on requests for footage.

20.2 Photographs and video

The school tells parents how it uses photographs of pupils and seeks written consent before using images in publications, on the website, on social media, or in recordings of school events. Consent can be withdrawn at any time.

Images taken by parents for personal and family use, for example at a school play, are not covered by data protection law. Parents are asked not to share images of other children on social media.

21. Data Retention and Disposal

Data is not kept for longer than necessary. The school documents the information it holds and disposes of it in line with its retention schedule, which is based on the Information and Records Management Society Records Management Toolkit for Schools.

- Some records about former pupils and staff are kept for extended periods for legal reasons or to provide references.
- Paper records are cross-cut shredded or pulped.
- Electronic records are securely deleted, and storage media are wiped or destroyed.
- A certificate of destruction is obtained when hard drives that held personal data are disposed of.

22. DBS Data

All data provided by the DBS is handled in line with data protection law. DBS certificates are not copied or kept for longer than six months. The school records the details required on the single central record. Any third party who accesses DBS information is made aware of their responsibilities.

23. Artificial Intelligence

Staff must not enter personal data about pupils, families or staff into any AI tool unless the tool is on the school's approved register and the use is permitted by the Safe Use of Artificial Intelligence (AI) Policy. Entering personal data into an unapproved tool is treated as a potential data breach.

24. Training

All staff and governors receive data protection training at induction and refresher training at least every two years, with updates when the law or school procedures change. Staff with particular responsibilities, such as the data protection lead, receive additional training.

25. Monitoring and Review

This policy is reviewed annually by the Headteacher with advice from the DPO, and approved by the Full Governing Body. It is reviewed sooner if there is a change in the law or guidance, or after a significant breach.