‘United through Jesus in Faith, Love and Learning’

POLICY – DATA PROTECTION

Office use only:

Date of Adoption:	MARCH 2026	Date of Review:	RECOOMEDNED ANNUALLY
Author:	J.MUDHURAPANTULA	Committee responsible for Review:	RESOURCES
Version:	1.0	APPROVED AT FGB 25.03.2026	

Contents

Aims & Objectives:

The aim of this policy is to provide a set of guidelines to enable all members of staff to understand:

- The law regarding personal data
- The importance of Personal Data governance
- How personal data should be processed, stored, archived and deleted/destroyed
- How staff, parents and pupils can access personal data
- Examples of good practices

The objective of the policy is to ensure that St Paul’s Catholic Primary School acts within the requirements of the Data Protection Act 2018 and General Data Protection Regulation (GDPR) when retaining and storing personal data, and when making it available to individuals.

St Paul’s Catholic Primary School recognises that protecting personal data is an expression of our commitment to uphold the dignity and rights of every individual created in the image of God.

This policy applies to all personal data, whether held in paper or electronic format, and to all members of the school community.

Data Protection – the law:

This policy meets the requirements of the:
• UK General Data Protection Regulation (UK GDPR)
• Data Protection Act 2018
• Protection of Freedoms Act 2012 (where biometric data is used)
• The Education (Pupil Information) (England) Regulations 2005

It is based on guidance from the Information Commissioner’s Office (ICO) and the Department for Education (DfE).

Responsibility for Data Protection

The Governing Board is the Data Controller and has overall responsibility for ensuring that the school complies with data protection legislation.

The Headteacher acts as the representative of the Data Controller on a day-to-day basis.

The school's Data Protection Officer (DPO) is responsible for:
• monitoring compliance
• advising on data protection matters
• reporting annually to governors
• being the first point of contact for the ICO and data subjects.

The school's Data Protection Officer (DPO) is provided by [insert organisation], and is contactable via [email].

The 7 principles of the Data Protection Act 2018

The UK GDPR is based on the following principles. Personal data must be:

1. Processed lawfully, fairly and transparently
2. Collected for specified, explicit and legitimate purposes
3. Adequate, relevant and limited to what is necessary
4. Accurate and kept up to date
5. Kept for no longer than is necessary
6. Processed securely
7. Processed in line with the accountability principle

The importance of Personal Data governance:

The smooth running of a school involves a high level of trust amongst all members of the school community. When large amount of personal data is being stored in IT and paper-based systems set up by the school, data protection is an important responsibility for all members of staff.

There are many benefits: - imagine the time a school can save from sharing a well organised archive where teachers can search for pupil data easily; imagine the reputational damage a school would suffer from when ransomware manages to get onto a school system and have to pay a large sum of money or suffer from days of system outage?

Fair processing of personal data: data which may be shared

Schools, local education authorities and the Department for Education (DfE) all hold information on pupils in order to run the education system, and in doing so have to follow the Data Protection and related Acts. This means, among other things, that the data held about pupils must only be used for specific purposes allowed by law. The school has a Fair Processing or Privacy Notice which explains how personal data is used and with whom it will be shared. This Notice is published here:

https://www.stpauls.w-berks.sch.uk/attachments/download.asp?file=1454&type=pdf

Lawful basis for processing personal data

The school will only process personal data where it has a lawful basis to do so in accordance with UK GDPR. In most cases, the processing of personal data by the school is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the school. This includes the provision of education, safeguarding and promoting the welfare of children, and the administration and management of the school.

Personal data may also be processed where it is necessary for the school to comply with a legal obligation, where it is required to fulfil a contract, or where it is necessary to protect the vital interests of an individual. In limited circumstances, the school may rely on legitimate interests, provided that the rights and freedoms of the individual are not overridden. Where none of these lawful bases apply, the school will seek the consent of the individual before processing their personal data.

Where the school processes special category data, such as information relating to health, ethnicity, religion, safeguarding or special educational needs, an additional condition for processing will be met in accordance with data protection legislation.

Staff must consult the Data Protection Officer if they are unsure about the lawful basis for processing personal data.

Processing, storing, archiving and deleting personal data: guidance

- The school will ensure that all personal data is processed securely and in accordance with the data protection principles. Appropriate technical and organisational measures will be in place to protect personal data against unauthorised or unlawful access, alteration, disclosure or destruction. These measures will include secure storage, controlled access, encryption where appropriate, and the secure transfer of data.
- Personal data and school records about pupils are confidential to the child. The information can be shared appropriately within the professional working of the school to enable the school to make the best educational provision for the child. The law permits such information to be shared with other educational establishments when pupils change schools.

Educational records for a child are kept for seven years after the child leaves the school unless subject to legal hold and or for children with special educational needs. Pictures of children, unless constitute as part of an educational record and filed accordingly, will not be kept beyond the end of the related school year. Official records of nativity public performance will be kept for a maximum of three years.

- Data on staff is sensitive information and confidential to the individual. It is only shared, where appropriate, at the discretion of the Head Teacher and with the knowledge, and if possible the agreement of the staff member concerned. This include data on school-provided e-mail system.

- Employment records form part of a staff member's permanent record. Because there are specific legislative issues connected with these (salary and pension details etc.) these records should be retained as set out by the Local Authority (http://www.westberks.gov.uk/retention)

- Interview records, CVs and application forms for unsuccessful applicants are kept for 6 months.

- All formal complaints made to the Head Teacher or School Governors will be kept for at least seven years in confidential files, with any documents on the outcome of such complaints. Individuals concerned in such complaints may have access to such files subject to data protection and to legal professional privilege in the event of a court case.

- All members of staff should only access school-provided systems (including e-mail) up to the last day of employment. Where personal data is taken off site, this must be done securely and in line with the school's data security procedures.

- All staff should notify any data breaches or near misses to the data protection co-ordinator in the school office, the DPO (Contact details on school website). All data breaches will be managed in accordance with the school's data breach procedure and, where required, reported to the Information Commissioner's Office within 72 hours.

- All confidential data will be disposed of securely in accordance with the school's records retention schedule and data protection legislation.

Accessing personal data: guidance

- A child can request access to his/her own data. The request is not charged and does not have to be in writing. Subject access requests may be made verbally or in writing and must be forwarded immediately to the Data Protection Officer. The staff will judge whether the request is in the child's best interests, and that the child will understand the information provided. They may also wish to consider whether the request has been made under coercion. All decisions should be documented.

- A parent can request access to or a copy of their child's school records and other information held about their child. The request must be made in writing. There is no charge for such requests on behalf of the child, but there may be an agreed charge for photocopying existing non-digital records. Staff should check, if a request for information is made by a parent, that no other legal obstruction (for example, a court order limiting an individual's exercise of parental responsibility) is in force. The school may request proof of identity before disclosing personal data to ensure that information is only released to authorised individuals.

- Parents should note that all rights under the Data Protection Act to do with information about their child rest with the child as soon as they are old enough to understand these rights. This will vary from one child to another, but, as a broad guide, it is reckoned that most children will have a sufficient understanding by the age of 12. Parents are encouraged to discuss and explain any request for information with their child if they are aged 12 or over.

- Separately from the Data Protection Act, The Education (Pupil Information) (England) Regulations 2005 provide a pupil's parent (regardless of the age of the pupil) with the right to view, or to have a copy of, their child's educational record at the school. Parents who wish to exercise this right must apply to the school in writing.

- For educational records (unlike other personal data; see below) access must be provided within 15 school days, and if copies are requested, these must be supplied within 15 school days of payment of the cost of copying.

- A member of staff can request access to their own records at no charge, but the request must be made in writing. The member of staff has the right to see their own records, and to ask for copies of the records. There is no charge for copies of records.

- Under UK GDPR, the school will respond to subject access requests without undue delay and within one calendar month of receipt. In cases where requests are complex or numerous, this period may be extended by a further two months and the individual will be informed. All requests will be acknowledged in writing on receipt, and access to records will be arranged as soon as possible. If awaiting third party consents, the school will arrange access to those documents already available and notify the individual that other documents may be made available later. Individuals have the right to complain to the Information Commissioner's Office if they are dissatisfied with the way their request has been handled.
- In all cases, should third party information (information about another individual) be included in the information the staff will try to obtain permission from the third party to show this information to the applicant. If third party permission is not obtained the person with overall responsibility should consider whether the information can still be released.

- Personal data should always be of direct relevance to the person requesting the data. A document discussing more general concerns may not be defined as personal data.

- Under the Freedom of Information Act, a request for personal information can include unstructured as well as structured records – for example, letters, emails etc. not kept within an individual's personal files, or filed by their name, but still directly relevant to them. If these would form part of a wider record it is advisable to file these within structured records as a matter of course and to avoid excessive administrative work in the future.

- Anyone who requests to see their personal data has the right to question the accuracy of matters of fact within the data, and to ask to have inaccurate information deleted or changed. They may also question opinions, and their comments will be recorded, but opinions do not need to be deleted or changed as a part of this process.

- The school will document all requests for personal information with details of who dealt with the request, what information was provided and when, and any outcomes (letter requesting changes etc.) This will enable staff to deal with a complaint if one is made in relation to the request.

Personal Data Breaches

The school will make all reasonable endeavours to ensure that personal data is kept secure and that data breaches do not occur.

Any actual or suspected data breach must be reported immediately to the Data Protection Officer. The school will investigate the breach, take appropriate steps to contain and minimise the risk, and assess the potential impact on individuals.

Where required, the breach will be reported to the Information Commissioner's Office within 72 hours of the school becoming aware of it. Individuals affected will be informed where there is a high risk to their rights and freedoms.

A record of all data breaches, including near misses, will be maintained and reviewed in order to improve practice and reduce the risk of future incidents.

Examples of good practices

All staff are responsible for ensuring that personal data is handled securely and in accordance with this policy at all times.

- Only school-provided data storage (which are centrally archived/encrypted) should be used to store work-related personal data. No USB pen is to be used for storing personal data.
- Avoid using unknown suppliers of WiFi services for work activities which involves personal data.
- Do not open uninvited e-mail from unrecognised source – check its source with a phone call or delete the mail item without opening any attachment / click on any links.
- Only use computers which have operational anti-virus software.
- Use [secure] e-mail tool by default for all communication involving personal data.
- Look out for unexpected behaviour of your computer – if in doubt, check with a colleague.
- Log queries as questions for your next CPD – everything has an explanation.
- Work to separate (storage of) personal and non-personal data as and when data are being worked on.
- Get to know the steps you need to follow when personal data is lost / leaked to the open world.
- Practice what we preach – children would pick up good practices from us – it is their future we are working to safeguard.
- Personal data must not be entered into unauthorised artificial intelligence tools or applications. Any such use will be treated as a data breach.

All staff and governors will receive data protection training as part of their induction and through regular updates.

The Data Protection Officer will monitor compliance and provide an annual report to the Governing Board.

This policy will be reviewed annually.