Data Protection Policy
St Mary's Catholic Primary School

Reviewed: September 2026

Love, Listen and Learn

Mission Statement

St. Mary's school community follows the teachings of Jesus Christ, working together to develop the whole child, in a spiritual, moral, academic, physical, social and emotional way, within a caring and supportive environment.

Ethos

We recognise that there is a challenge in creating an enriching environment for all those involved at every level of school life. We take our lead and inspiration from Christ with regard to the Gospel values: the belief that all human beings are uniquely created and loved by God and worthy of respect. This challenge manifests itself in the way we treat and value:

- Our relationships with each other and the wider community
- Our respect for one another
- Our welcome to and interest in all those who visit our school
- Discipline inspired by healing, forgiveness and reconciliation
- Our school environment

Through rising to this challenge we aim to create an awareness of a sense of belonging to and being part of the life at St Mary's.

The school follows the London borough of Enfield procedures.

Contents

1 **Introduction** 3
2 **Definitions** 3
3 **Scope of the Policy** 4
4 **Data Protection Principles** 4
5 **Lawful Basis for Processing** 5
6 **Data Collection** 6
7 **Data Sharing and Processing** 7
8 **Retention and Disposal** 7
9 **Security** 7
10 **Individual Rights** 8
11 **Data Breaches** 8
12 **Smart Glasses/Wearable Devices** 9
13 **Complaints** 9
14 **Policy Review** 10

1 Introduction

1.1 As part of our information governance responsibilities, we must ensure that appropriate controls are in place to govern the collection, use, storage, sharing, and retention of personal information relating to pupils, parents, staff and contractors, and visitors These controls must comply with the requirements of current data protection legislation, in particular the Data Protection Act 2018, the UK GDPR Act, and the Data Use and Access Act 2025.

1.2 This policy provides a framework to help staff meet the school's legal and organisational responsibilities when handling personal information. It applies to all personal data that is created, collected, received, stored, used, shared or disposed of by the school, regardless of the format in which it is held or where it is stored.

2 Definitions

Personal Data

2.1 Any information relating to an identified or identifiable individual. A person may be identified directly from the information itself or indirectly when that information is combined with other data that the school holds or can reasonably obtain. Personal data includes both special category personal data and pseudonymised data where an individual can still be identified. It does not include anonymous information where the identity of an individual has been permanently removed and can no longer be determined.

2.2 Personal data can be information, such as a name, address, email address, date of birth or location data. It can also include opinions, assessments or records relating to an individual's actions, behaviour, performance, or circumstances.

Data Subject

2.3 An individual about whom personal information is stored is known as the Data Subject. It includes, but is not limited to pupils, parents, staff and contractors, and visitors.

Special Category Personal Data

2.4 Personal information relating to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health, sex life, sexual orientation, biometric data or genetic data.

2.5 Before special category personal data is processed, the school will ensure that an appropriate assessment has been carried out to confirm that the proposed processing meets the relevant legal requirements. Individuals will also be informed, through a privacy notice, consent process, or other appropriate communication about the nature of the processing, the purposes for which their information will be used, and the legal basis being relied upon. The school will only process special category personal data where there is a clear lawful basis for doing so and where the additional conditions required under data protection legislation have been satisfied. Appropriate safeguards will be applied to ensure that this information is handled securely and only accessed by authorised individuals with a legitimate need to do so.

Criminal Offence Data

2.6 Refers to personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.

Scope of the Policy

2.7 The purpose of this policy is to clarify the school's legal obligations when processing personal data and to ensure that all personal information is:

- Collected, stored and processed only for legitimate school purposes.
- Processed on an appropriate lawful basis, or with valid consent where required.
- Accessed only by individuals with a legitimate need to do so.
- Kept secure and protected from unauthorised access, loss or misuse.
- Retained only for as long as necessary and in accordance with retention requirements.
- Shared only with authorised individuals or organisations, with appropriate records of disclosure maintained

2.8 Through these measures, the school seeks to protect the privacy and rights of individuals while ensuring that personal information is managed responsibly, securely, and in accordance with legal requirements.

2.9 This policy applies to all members of the school workforce, including employees, agency workers, volunteers, contractors, consultants and any other person who handles personal data on behalf of the school. Protecting personal information is a shared responsibility, and all staff are expected to comply with this policy and support the school's data protection obligations.

Responsibilities

2.10 During their employment, staff may have access to the personal information of other members of staff, pupils, parents and guardians, suppliers, or the public. The school expects staff to help meet its data protection obligations to those individuals.

2.11 If you have access to personal information, you must:

- Only access the personal information that you have authority to access and only for authorised purposes.
- Only allow other staff to access personal information if they have appropriate authorisation.
- Only allow individuals who are not school staff to access personal information if you have specific authority to do so and there is legal basis for doing so.
- Keep personal information secure by complying with rules on access to premises, computer access, password protection and secure file storage and destruction in accordance with the school's policies.
- Do not remove personal information, or devices containing personal information, from the school's premises unless appropriate security measures are in place to secure the information and the device
- Do not store personal information on local drives or on personal devices that are used for work purposes.

3 Data Protection Principles

3.1 The UK GDPR sets out key principles that must be followed whenever personal data is processed. Processing includes activities such as collecting, recording, storing, using,

sharing, and deleting personal information. All staff who handle personal data as part of their role are responsible for ensuring that these principles are always applied.

3.2 Under Article 5 of the UK GDPR, personal data must be:

- Processed lawfully, fairly and transparently, so that individuals understand how and why their information is being used.
- Collected for specified, explicit and legitimate purposes, and not used in ways that are incompatible with those original purposes.
- Adequate, relevant and limited to what is necessary for the purpose for which it is being processed.
- Accurate and kept up to date where necessary, with reasonable steps taken to correct or delete inaccurate information without undue delay.
- Retained only for as long as necessary to fulfil the purposes for which it was collected and processed.
- Processed securely, with appropriate technical and organisational measures in place to protect personal data from unauthorised or unlawful access, accidental loss, destruction or damage, and to safeguard the rights and freedoms of individuals.
- Managed in accordance with the principle of accountability, meaning that the school must be able to demonstrate its compliance with data protection legislation and maintain appropriate records, policies, procedures and controls.

3.3 These principles form the foundation of our approach to data protection and must be considered whenever personal data is collected, used, shared, stored or disposed of.

3.4 The Information Commissioner (ICO) administers Data Protection in the UK and further information on the principles can be found on the ICO website.

4 Lawful Basis for Processing

4.1 Before commencing any new processing activity, and periodically thereafter, the school must identify and document the purpose of the processing and determine the most appropriate lawful basis under the UK GDPR.

4.2 The lawful basis selected must accurately reflect the nature and purpose of the processing and be recorded where required. Staff must ensure that personal data is only processed where a valid lawful basis applies and that the chosen basis is reviewed if the purpose of the processing changes. Lawful bases include:

- Processing 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.
- Processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the data controller is subject.
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
- Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party.

- The data subject has given consent to the processing of their data for one or more specific purposes.

4.3 The decision as to which lawful basis applies must be documented, to demonstrate compliance with the data protection principles, and include information about both the purposes of the processing and the lawful basis for it in the school's relevant privacy notices.

5 Data Collection

5.1 The school collects, uses and maintains personal data from a variety of sources, including information provided directly by individuals, such as pupils, parents, staff, contractors and other data subjects. Personal data may also be obtained from third parties where there is a lawful basis for doing so and where such collection is necessary to support the school's functions and responsibilities.

5.2 In some circumstances, personal data may be collected indirectly via monitoring and security systems. This includes, but is not limited to, door access control systems, CCTV, visitor management systems, physical security logs and other electronic monitoring technologies. The use of such systems is subject to appropriate safeguards and is carried out in accordance with the school's information governance and security requirements.

5.3 Categories of information that we collect, hold and/or share include, but are not limited to:

- Personal data.
- Special category personal data.
- Characteristics, such as free school meal eligibility or Pupil Premium Information.
- Safeguarding information, such as court orders and professional involvement.
- Medical data, such as doctor information, health, allergies, medication, and dietary requirements.
- Attendance information.
- Assessment information and attainment
- Special Educational Needs information, including needs.
- Behavioural information, such as exclusions and any relevant alternative provision put in place.
- Financial Information, such as dinner money transactions and trip transactions.

5.4 We use this data to:

- Support pupil learning.
- Monitor and report on pupil attainment progress.
- Provide appropriate pastoral care.
- Assess the quality of our services.
- Keep children safe.
- Meet the statutory duties placed on us by the Department for Education.
- Comply with the law regarding data sharing.
- Complete financial audits.

6 Data Sharing and Processing

6.1 Schools are required to routinely share personal data with authorities, partners and service providers, including, but not limited to:

- Other schools that pupils attend after leaving us.
- The London Borough of Enfield and other relevant local authorities.
- The Department for Education.
- The NHS.

6.2 Where personal information is shared with, or processed by, a third party, the school will ensure that appropriate agreements and controls are in place to support lawful, secure and transparent processing. Arrangements for sharing or processing personal data will be documented, regularly reviewed and monitored to ensure compliance with data protection legislation and to safeguard the information being handled.

6.3 All sharing of personal data with third parties must be supported by an appropriate written agreement. Where personal data is shared with another organisation for its own purposes, or where the school and another organisation jointly determine how the data will be used, a *Data Sharing Agreement* must be in place.

6.4 Requests for personal data from the Police or other law enforcement agencies may be considered where there is a legitimate purpose, such as safeguarding or the prevention and detection of crime. The school is not normally required to disclose information and must be satisfied that any request is lawful, necessary, and proportionate. The requesting agency must provide sufficient information to explain why the data is required and how non-disclosure could prejudice an investigation.

6.5 Requests should be made formally in writing and authorised by a senior officer. Any disclosure must be approved by the school, and a record must be kept of the information shared, the legal basis relied upon, and the reasons for the disclosure.

7 Retention and Disposal

7.1 The school must ensure that personal information is not kept for any longer than is necessary. This is to adhere to any legal, regulatory or specific business justification. The school will retain some forms of information longer than others, but all decisions are to be based upon business requirements details can be found in the school's record retention schedule. Out retention criteria will be imposed on third parties with whom data is shared.

8 Security

8.1 The school will use appropriate technical and organisational measures to keep personal information secure, to protect against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

8.2 We will develop, implement and maintain safeguards appropriate to our size, the amount of personal data that we hold and process, or maintains on behalf of others. We will regularly evaluate and test the effectiveness of those safeguards to ensure security of processing.

8.3 Please note that:

- All staff are responsible for keeping information secure in accordance with legislation and must follow our acceptable usage policy.
- Staff must guard against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data.
- Staff must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use, or disclosure.
- Staff must follow all procedures and technologies put in place to maintain the security of all personal data from the point of collection to the point of destruction.
- Staff may only transfer personal data to third-party service providers who agree in writing to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

8.4 Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards the school has implemented and maintains.

9 Individual Rights

9.1 Data Subjects have the following rights in relation to their personal information:

- To be informed about how, why, and on what basis that information is processed.
- To obtain confirmation that personal information is being processed and to obtain access to it and certain other information, by making a Subject Access Request.
- To have data corrected if it is inaccurate or incomplete.
- To have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (known as '*the right to be forgotten*').
- To restrict the processing of personal information where the accuracy of the information is contested, or the processing is, or where the school no longer need the personal information, but you require the data to establish, exercise or defend a legal claim.
- In limited circumstances, to receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format.
- To withdraw consent to processing (*if applicable*).
- To object to decisions based solely on automated processing, including profiling.
- To be notified of a data breach which is likely to result in *high risk* to their rights and obligations.
- To make a complaint to the Information Commissioner or a Court.

10 Data Breaches

10.1 A data breach is a security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data that has been transmitted, stored or otherwise processed. Data breaches can occur for a variety of reasons, including cyber-attacks, malicious actions by individuals, human error, system failures, or accidental exposure of information.

10.2 Personal data breaches can take many forms. Examples include, but are not limited to:

- Sending personal data to the wrong recipient, for example where information relating to a pupil is accidentally sent to the wrong parent or guardian.
- Access to personal data by an unauthorised third party.
- Deliberate or accidental actions, or failures to act that result in personal information being compromised.
- The loss or theft of devices containing personal data, such as laptops, mobile phones, USB drives, or paper records.
- The unauthorised alteration, deletion or corruption of personal data.

10.3 Personal data breaches can have serious consequences for the individuals affected. The unauthorised disclosure of sensitive information, such as health, safeguarding or other confidential personal data, may result in financial loss, emotional distress, reputational damage or other harm to pupils, their families, staff or other individuals.

10.4 Data breaches can also damage the school's reputation and reduce trust among pupils, parents, staff and the wider community. Maintaining strong data protection practices is therefore essential to protect individuals, meet legal obligations and maintain confidence in the school's ability to safeguard personal information.

11 Smart Glasses/Wearable Devices

11.1 As technology continues to evolve, new devices are reshaping the way we connect, learn, and share information. One of the latest innovations is Smart Glasses; eyewear that looks like ordinary spectacles but can include built-in cameras, microphones, and internet connectivity.

11.2 Smart glasses can discreetly record, live-stream, or share content instantly, and therefore can pose risks to pupils, staff, and visitors. In response to this, and to ensure our community remains a safe and secure place, the use of smart glasses, and similar wearable devices, will not be permitted on school grounds by pupils, parents, visitors, or staff.

12 Complaints

12.1 Individuals have the right to make a complaint to the school if they believe their data protection rights have been breached. We acknowledge complaints within 30 days, but our aim is to do better than this statutory minimum and deal with such complaints in the same timescales as our existing complaints procedure.

12.2 However, should investigations require a longer timeframe than set out in the complaints policy we commit to ensuring that investigations are completed without undue delay and that we will keep individuals informed of progress, as per our legal obligation.

12.3 If you have raised a data protection complaint our final review will remind you that if you remain dissatisfied your right to escalate the matter to the ICO. Under the Data Use

and Access Act 2025, the ICO will generally expect you to complete the internal complaints process before it will investigate.

The ICO contact details are:

Post: *Information Commissioner's Office,*
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire,
SK9 5AF

Tel: *0303 123 1113*

Web: *www.ico.org.uk*

13 Policy Review

13.1 This policy will be reviewed annually by the senior leadership team and updated as necessary to reflect changes in technology, emerging cyber security threats, legal and regulatory requirements, and recognised best practice.

13.2 Any revisions to the policy will be submitted to the Board of Governors for approval. The Board of Governors is also responsible for providing strategic oversight of the school's cyber security arrangements and for ensuring appropriate assurance is in place regarding compliance with this policy and related security requirements.