Data Protection Policy
2025

Through Christ we believe, inspire, achieve.

Completed by: Fiona Delaney
Last Updated: July 2025
Agreed by Governors: July 2025
Next Updated: July 2026

1. Rationale

English Martyrs Catholic Primary School is required to keep certain personal data about its staff and pupils in order to fulfil its purpose and to meet its legal obligations to funding bodies and government. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) , the The Data Protection, Privacy and Electronic Communications (Amendments) (EU Exit) Regulations 2020 and the provisions of the Data Protection Act 2018 (DPA 2018).

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

All members of staff at English Martyrs Catholic Primary School have been provided with Data Protection and GDPR awareness training and will receive annual refresher training alongside any training/information updates as and when deemed appropriate to ensure the ongoing best practice in data protection in the school. The policy is communicated to all staff via the staff drive. Staff are expected to understand and abide by this policy. Any breach of this policy will be taken seriously and may result in formal action being taken.

Any member of staff, parent/carer or pupil who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with the Data Protection Lead. External stakeholders have access to this policy via the school website.

2. Equal Opportunities

Inclusion is at the centre of everything we do at English Martyrs. We recognise the varying needs of all our learners, staff, governors and visitors and so differentiate where necessary and as appropriate. Equal opportunities will be given to all children, staff, governors and visitors in respect of:

- Race
- Gender
- Culture
- Special Educational Needs

3. Legislation and Guidance

This policy meets the requirements of the GDPR and DPA 2018 and amendments of The Data Protection, Privacy & Electronic Communications (amendments etc) (EU Exit) Regulations 2020. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

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.

4. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: ● Name (including initials) ● Identification number ● Location data ● Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: ● Racial or ethnic origin ● Political opinions ● Religious or philosophical beliefs ● Trade union membership ● Genetics ● Health – physical or mental ● Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

5. The Data Controller

English Martyrs Catholic Primary School processes personal data relating to parents, pupils, staff, governors, visitors and others, and is, therefore, a data controller and responsible for implementation. As a Data Controller, the school must 'notify' (register with) the Information Commissioner's Office (ICO) under the GDPR annually. English Martyrs Catholic Primary School

is registered with the ICO under reference **Z7384462** and has paid its data protection fee to the ICO, as legally required. The registration certificate expires on 17th November 2026 and will be renewed in a timely manner.

If you have any questions regarding Data Protection at School, please contact the Data Protection Lead Mrs Delaney on 928 5601.

6. Roles and Responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

6.1. Governing Body

The School is a registered Data Controller and Governors hold overall responsibility to ensure that our school complies with all relevant data protection obligations and that:

- the policy is reviewed every two years (in line with statutory requirements).
- the policy is clearly communicated, implemented and monitored by the school.

6.2. Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. They will provide an annual report of their activities directly to the Governing Body and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO. Our DPO is **Mrs Mairead O'Neill Dowell** and is contactable on 0151 928 5601 or via email on data@englishmartyrs.co.uk.

6.3 Headteacher

The Headteacher acts as the representative of the data controller on a day-to-day basis and will ensure that:

- the policy is presented for review by Governors every two years (according to the requirements of the GDPR) and arrangements are reviewed by the school annually to ensure the policy reflects up to date best practice in data management, security and control.
- the policy is clearly communicated to all stakeholders and the school's obligations under the policy are fully met.
- the school complies fully with the GDPR and manages its information and records appropriately.

6.4 Data Protection Lead (DPL)

The Headteacher has designated a single point of contact for all matters relating to data protection in English Martyrs Catholic Primary School known as the Data Protection Lead (DPL). See contact details above.

The DPL will ensure that:

- the school complies fully with the GDPR and manages its information and records appropriately.

- the school provides clear communication to stakeholders about what/why personal data is collected and details of any sharing of information. The school will do this via 'Privacy Notices' which will be issued to stakeholders annually.
- all staff who are responsible for handling personal data are fully aware of, and understand, the school's obligations and receive the appropriate training.
- the school registers with the Information Commissioner's Office (ICO) annually, providing or updating the school's 'notification'.
- the school shares information with others only when it is legally appropriate to do so or where explicit consent has been received by the data subject.
- personal information is not retained for longer than is necessary and that when obsolete information is destroyed, it is done so appropriately and securely.
- procedures are in place to ensure compliance with the duty to respond to requests for access to personal information, known as 'Subject Access Requests' (SAR).
- all necessary precautions are in place to protect against physical loss or damage, and that both access and disclosure is restricted, irrespective of the format in which it is recorded.

6.5 All Staff

Data Protection is a responsibility of all staff at English Martyrs Catholic Primary School. All staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPL/DPO in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - If they have any concerns that this policy is not being followed
  - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
  - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
  - If there has been a data breach
  - Whenever they are engaging in a new activity that may affect the privacy rights of individuals

If they need help with any contracts or sharing personal data with third parties

7. Data Protection Principles

The GDPR is based on compliance with the following data protection principles requiring that data is:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date

- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

8. Collection Personal Data

8.1 Lawfulness, fairness and transparency

We will only process personal data where we have **one** of **six** 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given explicit consent
- The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent.
- The data has already been made manifestly public by the individual
- The data needs to be processed for the establishment, exercise or defence of legal claims
- The data needs to be processed for reasons of substantial public interest as defined in legislation
- The data needs to be processed for health and social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for public health reasons, and the processing is done by, or under the direction of , a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for archiving purposes, scientific or historical research purposes or statistical purposes and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given consent
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual

- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice or for the establishment, exercise or defence of legal rights
- The data needs to be processed for reasons of substantial public interest as defined in legislation

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

8.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

We will keep data accurate and where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's Record Retention Schedule.

9. Sharing Personal Data

We will not normally share personal data with anyone else, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils for example, IT companies. When doing this, we will:
  - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
  - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
  - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data internationally, we will do so in accordance with data protection law.

10. Subject Access Requests (SAR) and other Rights of Individuals

10.1 Subject Access Requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form but we may be able to response to requests more quickly if they are made in writing and include:Name of individual

- Name of Individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO.

10.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupils' ability to understand their rights will always be judged on a case-by-case basis.

10.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide two forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge unless the request is substantial and or complicated
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests (Safeguarding)
- Would include another person's personal data that we can't reasonably anonymise and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references or exam scripts

If the request is unfounded or excessive, we may refuse to act on it or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

10.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
-
- Challenge decisions based solely on automated decision making or profiling (i.e making decisions or evaluating certain things about an individual based on their personal data no human involvement)
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

11 Parental requests to see the Education record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

If the request is for a copy of the education record, the school may charge a fee to cover the cost of supplying it.

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual or if it would mean releasing exam marks before they are officially announced.

12. Biometric Recognition Systems

These systems are not currently used by school. Parent/carers will be notified before any biometric recognition system is put in place or before their child takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it. Further information will be shared with parents if school moves to any such system and this policy will be updated in line with relevant legislation at that point.

13. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

The CCTV system is in operation to 'Detect & Prevent Crime and for Safety'.

Any enquiries about the CCTV system should be directed to **Mrs Delaney**, **Office Manager**.

14. Photographs and Videos

As part of our school activities, we may take photographs and record images of individuals within our school. We will obtain written consent from parents/carers, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to the parent/carer.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we only use the forename of the pupil. Please refer to our Child Protection Policy for further information.

15. Artificial Intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such a ChatGPT and Google Bard. English Martyrs recognises that AI has many uses to help pupils learn, but also pose risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, English Martyrs will treat this as a data breach and will follow the personal data breach procedure outlined in this policy.

16. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws will apply
- Maintaining records of our processing activities, including:
  - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
  - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

17. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use.
- Papers containing confidential personal data must not be left on office and classroom desks, on staff room tables, pinned to notice/display boards, or left anywhere else where there is general access.
- Where personal information needs to be taken off site permission will be sought from the Head Teacher or DPL.
- A strong password policy is in place to protect access to school hardware and IT infrastructure. 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 and Governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see E Safety Policy and Child Protection Policy).

- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

18. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use an accredited third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

19. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1. All data breaches will be recorded and shared with our DPO. When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it.

20. Training

All staff and Governors 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, guidance or the school's processes make it necessary. The Data Lead will ensure staff are regularly updated and reminded of Data Protection issues.

21. Links with other policies

This policy should be read in conjunction with the following school policies:

- Child Protection Policy
- Freedom of Information Policy
- E-Safety Policy
- Records of Retention Schedule
- Privacy notices

22. Monitoring of the Policy

This policy will be monitored annually in line with the 'School Policy Review Chart' or as and when government legislation is updated. Changes will be reported to the Full Governing Body for approval.