ENGLISH MARTYRS CATHOLIC PRIMARY SCHOOL
DATA PROTECTION POLICY
(BASED ON WSCC MODEL POLICY)

Date of Approval	**March 2025**
Date of Next Review	**March 2027**
Review led by	**Headteacher**
Approved by	**Full Governing Body**
This Policy should be read in conjunction with the following documents	• **Staff Code of Conduct** • **Complaints Policy** • **Equality information and objectives** • **Privacy Notice** • **Acceptable IT use**
Notes	

School Mission Statement
Our Mission statement demonstrates our commitment to inclusion at English Martyrs school:

To accept each individual as they are and to enable them to develop their full potential within a Christ-centred, worshipping community in a spirit of love, happiness and understanding

'A *Learning Community in Christ*'

Introduction

On the 25th May 2018 the General Data Protection Regulation (GDPR) will be applicable and the current Data Protection Act (DPA) will be updated by a new Act giving effect to its provisions. Before that time the DPA will continue to apply.

This Policy sets out the manner in which personal data of staff, students and other individuals is processed fairly and lawfully.

The School collects and uses personal information about staff, students, parents or carers and other individuals who come into contact with the School. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the School complies with its statutory obligations.

The School is a data controller and must therefore comply with the Data Protection Principles in the processing of personal data, including the way in which the data is obtained, stored, used, disclosed and destroyed. The School must be able to demonstrate compliance. Failure to comply with the Principles exposes the School and staff to civil and criminal claims and possible financial penalties.

Details of the School's purpose for holding and processing data can be viewed on the data protection register: https://ico.org.uk/esdwebpages/search

The Schools registration number is Z7368077. This registration is renewed annually and up dated as and when necessary.

Aim

This Policy will ensure:

The School processes person data fairly and lawfully and in compliance with the Data Protection Principles.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities under this policy.

That the data protection rights of those involved with the School community are safeguarded.

Confidence in the School's ability to process data fairly and securely.

Scope

This Policy applies to:

Personal data of all School employees, governors, students, parents and carers, volunteers and any other person carrying out activities on behalf of the School.

The processing of personal data, both in manual form and on computer.

All staff and governors.

The Data Protection Principles

The School will ensure that personal data will be:

1. Processed fairly, lawfully and in a transparent manner.

2. Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes.

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which data is processed.

4. Accurate and, where necessary, kept up to date.

5. Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

6. Processed in a way that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The School will be able to demonstrate compliance with these principles.

The School will have in place a process for dealing with the exercise of the following rights by Governors, staff, students, parents and members of the public in respect of their personal data:

- to be informed about what data is held, why it is being processed and who it is shared with;
- to access their data;
- to rectification of the record;
- to erasure;
- to restrict processing;
- to data portability;
- to object to processing;
- not to be subject to automated decision-making including
- profiling.

Roles and Responsibilities

The Governing Body of the School and the Head Teacher are responsible for implementing good data protection practices and procedures within the School and for compliance with the Data Protection Principles.

It is the responsibility of all staff to ensure that their working practices comply with the Data Protection Principles. Disciplinary action may be taken against any employee who breaches any of the instructions or procedures forming part of this policy

~~A designated member of staff,~~ The Data Protection Officer, will have responsibility for all issues relating to the processing of personal data and will report directly to the Head Teacher.

The Data Protection Officer will comply with responsibilities under the GDPR and will deal with subject access requests, requests for rectification and erasure, data security breaches. Complaints about data processing will be dealt with in accordance with the Schools Complaints Policy.

Data Security and Data Security Breach Management

All staff are responsible for ensuring that personal data which they process is kept securely and is not disclosed to any unauthorised third parties.

Access to personal data should only be given to those who need access for the purpose of their duties.

All staff will comply with the Schools Acceptable IT use Policy.

Staff who work from home must have particular regard to the need to ensure compliance with this Policy and the Acceptable IT use Policy.

Data will be destroyed securely in accordance with the 'Information and Records Management Society Retention Guidelines for Schools'.

New types of processing personal data including surveillance technology which are likely to result in a high risk to the rights and freedoms of the individual will not be implemented until a Privacy Impact Risk Assessment has been carried out (Appendix B).

The School will have in place a data breach security management process and serious breaches where there is a high risk to the rights of the individual will be reported to the Information Commissioner's Office (ICO) in compliance with the GDPR.

All staff will be aware of and follow the data breach security management process.

All staff will be aware of and comply with the list of Do's and Don'ts in relation to data security in Appendix A

Subject Access Requests

Requests for access to personal data (Subject Access Requests) (SARs) will be ~~processed~~ overseen by the Data Protection Officer. Those making a Subject

Access Request will be charged a fee in accordance with Regulations. Generally, no fee is applicable. Records of all requests will be maintained.

The School will comply with the statutory time limits for effecting disclosure in response to a Subject Access Request. The statutory time period is one calendar month of receipt of the request.

Sharing data with third parties and data processing undertaken on behalf of the School.

Personal data will only be shared with appropriate authorities and third parties where it is fair and lawful to do so. Any sharing will be undertaken by trained personnel using secure methods. Where a third party undertakes data processing on behalf of the School e.g. by providing cloud based systems or shredding services, the School will ensure that there is a written agreement requiring the data to be processed in accordance with the Data Protection Principles.

Ensuring compliance

All new staff will be trained on the data protection requirements as part of their induction.

Training and guidance will be available to all staff.

All staff will read the Acceptable IT use Policy.

The School advises students whose personal data is held, the purposes for which it is processed and who it will be shared with. This is referred to as a "Privacy Notice" and is available on the School website.

The School also provides a Privacy Notice to staff which is available on the School website.

The School will ensure Privacy Notices contains the following information:

- Contact Data Controller and Data Protection Officer
- Purpose of processing and legal basis. Retentions period. Who we share data with.
- Right to request rectification, erasure, to withdraw consent, to complain, or to know about any automated decision making and the right to data portability where applicable.

Photographs, Additional Personal Data and Consents

Where the School seeks consents for processing person data such as photographs at events it will ensure that appropriate written consents are obtained. Those consent forms will provide details of how the consent can be withdrawn.

Where the personal data involves a child under 16 years written consent will be required from the adult with parental responsibility.

Appendix A

What staff should do:

DO get the permission of your manager to take any confidential information home.
DO transport information from school on secure computing devices (i.e. encrypted laptops and encrypted memory sticks). Wherever possible avoid taking paper documents out of the office.
DO use secure portable computing devices such as encrypted laptops and encrypted USB memory sticks when working remotely or from home.
DO ensure that any information on USB memory sticks is securely deleted off the device, or saved on a School shared drive.
DO ensure that all paper based information that is taken of premises is kept confidential and secure, ideally in a sealed envelope which indicates a return address if misplaced.
DO ensure that any confidential documents that are taken to your home are stored in a locked drawer.
DO ensure that paper based information and laptops are kept safe and close to hand when taken out off premises. Never leave them unattended. Particular care should be taken in public places (e.g. reading of documentation on public transport).
DO ensure that when transporting paper documentation in your car that it is placed in the boot (locked) during transit.
DO return the paper based information to the School as soon as possible and file or dispose of it securely.
DO report any loss of paper based information or portable computer devices to your line manager immediately.
DO ensure that all postal and e-mail addresses are checked to ensure safe dispatch of information. When sending personal information by post the envelope should clearly state 'Private – Contents for Addressee only'.
DO ensure that when posting/emailing information that only the specific content required by the recipient is sent.
DO use pseudonyms and anonymise personal data where possible.
DO ensure that access to SIMS (or equivalent) is restricted to appropriate staff only, that leavers are removed in a timely manner and that generic user names such as 'Sysman' are disabled.

What staff must not do:

DO NOT take confidential information to an entertainment or public place such as a pub or cinema, whether held on paper or an electronic device. Any information must be taken to the destination directly and never left unattended during the journey.
DO NOT unnecessarily copy other parties into e-mail correspondence.
DO NOT e-mail documents to your own personal computer.
DO NOT store work related documents on your home computer.
DO NOT leave personal information unclaimed on any printer or fax machine.
DO NOT leave personal information on your desk over night, or if you are away from your desk in meetings.

DO NOT leave documentation in vehicles overnight.
DO NOT discuss case level issues at social events or in public places.
DO NOT put confidential documents in non-confidential recycling bins.
DO NOT print off reports with personal data (e.g. pupil data) unless absolutely necessary.
DO NOT use unencrypted memory sticks or unencrypted laptops

APPENDIX B: Data Protection Impact Assessment Template

A Data Protection Impact Assessment (DPIA) needs to be completed to ensure the school handles student, staff, family and anyone else's personal information safely and responsibly. This is important because schools collect and use data like names, addresses, and health information.

The need comes from the UK General Data Protection Regulation (GDPR), which states that a DPIA should be completed when starting new projects that could affect people's privacy. By doing this, schools can identify and fix any potential risks to keep everyone's data secure.

The requirement for a DPIA is outlined in Article 35 of the GDPR, which specifies that they must be conducted when data processing is likely to result in a high risk to the rights and freedoms of individuals, especially when using new technologies. By following this regulation, schools can ensure they are protecting their students' personal information effectively.

1. Project details

Project name	
Project description	
Project lead	
Go live date	

2. Purpose of the DPIA

Describe in detail the purpose of the DPIA and the data processing activities involved, including what data will be used.

3. Data protection principles

3.1 Lawfulness, fairness, and transparency

a. What is the legal basis for processing (Article 6) personal data?

b. What is the legal basis for processing (Article 9 or 10) sensitive data?

c. How will you ensure that individuals are informed about the processing of their data?

3.2 Purpose limitation

a. What are the specific purposes for which the data will be used?

b. How will you ensure that the data is not used for other purposes?

3.3 Data minimisation

a. What data is absolutely necessary for the project?

b. How will you ensure that only the minimum amount of data is collected and processed?

3.4 Accuracy

a. How will you ensure that the data is accurate and up-to-date?

b. What steps will you take to correct inaccurate data?

3.5 Storage limitation

a. How long will the data be kept?

b. What is your process for securely deleting data that is no longer needed?

3.6 Integrity and confidentiality (security)

a. What measures will you take to protect the data from unauthorized access, loss, or damage?

b. How will you ensure that data is processed securely?

3.7 Accountability

a. Who is responsible for ensuring GDPR compliance in this project?

b. What documentation will you maintain to demonstrate compliance with GDPR?

4. Data subject rights

a. How will you ensure that individuals can exercise their rights (e.g., access, rectification, erasure, restriction, data portability, objection)?

5. Risk assessment

Description of risk	High / Medium / Low	Mitigation (for High /Medium only)	Remaining risk (Medium / Low)

Add as many rows as required.

6. Consultation

a. Have you consulted with the Data Protection Officer and if so, what was the feedback?

b. Have you consulted with stakeholder, such as pupils, parents, local authority, and if so, what was the feedback?

c. If you have not consulted with anyone, why not?

7. Approval and sign-off

a. DPO approval

Name	
Signature/embedded approval email	
Date	

b. Head approval

Name	
Signature/embedded approval email	
Date	

APPENDIX C: Information Security Policy

Introduction

This policy is based upon the sixth principle of the UK General Data Protection Regulation (GDPR) which states organisations must protect the personal data, which it processes, against unauthorised loss by implementing appropriate technical and organisational measures. It has been written to reflect the ISO 27001 information security standard.

The policy should be read in conjunction with other documents including the Data Protection Policy, Information Risk Management Procedure, and the Data Protection Breach Reporting Procedure.

1. Scope

This policy applies to all EMCPS employees, any authorised agents working on behalf of the school, including temporary or agency employees, and third-party contractors.

Individuals who are found to infringe these policies knowingly or recklessly may face disciplinary action.

The policies apply to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper.
- Information or data stored electronically.
- Communications sent by post/courier or using electronic means such as email, fax, or electronic file transfer.
- Information or data stored on or transferred to removable media such as USB storage device or memory card.
- Information stored on portable computing devices including mobile phones, tablets, cameras, and laptops.
- Speech, voice recordings and verbal communications, including voicemail.
- Photographs and other digital images.

Access control

EMCPS will maintain control over access to the personal and confidential data that is processes.

These controls will differ depending on the format of the data and the status of the individual accessing the data. We will maintain an audit log detailing which individuals have access to which systems (both electronic and manual).

3.1 Manual filing systems

Access to manual filing systems will be controlled by a key management system. All files, which contain personal and confidential data, will be locked away in lockable storage units, such as a filing cabinet or a document safe, when not in use.

Keys to storage units will be locked in a pin-operated key safe. The School Business Manager will be responsible for giving individuals access to the key safe. Access will only be given to individuals who require it to conduct legitimate business functions.

3.2 Electronic systems

Access to electronic systems will be controlled through a system of user authentication. Individuals will be given access to electronic filing systems if required to conduct legitimate functions. Wherever possible a two-tier authentication system will be implemented across all electronic systems.

Usernames are deleted when an individual leaves the employment of the school.

3.3 Software and systems audit logs

EMCPS will ensure that all systems have inbuilt audit logs so that it can monitor what employees and users have accessed and what changes may have been made. Although this is not a preventative measure it ensures that the integrity of the data can be assured and deters individuals from accessing records without authorisation.

3.4 Data shielding

EMCPS does not allow employees to access the personal data of family members or close friends. Employees should declare, upon employment, whether they are aware of any family members or friends who are registered at the school.

3.5 External access

On occasions the EMCPS will need to allow individuals who are not employees of the school to have access to data systems. This could be, for example, for audit purposes, to fulfil an inspection, use of agency staff. The Head is required to authorise all instances of third parties having access to systems.

An access log, detailing who has been given access to what systems and who authorised the access, will be maintained by the school.

Physical security

EMCPS will maintain high standards of Physical Security to prevent unauthorised access to personal and confidential data. The school will maintain the following controls:

4.1 Clear desk policy

Individuals will not leave personal and confidential data on desks, or any other working areas, unattended and will use the lockable storage units provided to secure personal and confidential data when not in use.

4.2 Intruder alarm system

The school will maintain a security alarm system at its premises so that, when the premises are not occupied, an adequate level of security is still in operation.

4.3 Building access

External doors to the premises will be locked when the premises are not occupied. Only authorised employees will be key holders for the building premises. The School Business Manager will be responsible for authorising key distribution and will maintain a log of key holders.

4.4 Internal access

Internal areas, which are off limits to pupils and parents, will be kept locked.

4.5 Visitor control

Visitors will be required to sign in a visitor's book and state their name, who they are visiting and the time of arrival and departure. Visitors will be escorted throughout the school and will not be allowed to access restricted areas without employee supervision.

Environmental security

As well as maintaining high standards of physical security, to protect against unauthorised access to personal and confidential data, the school must also protect data against environmental and natural hazards such as power loss, fire, and floods.

It is accepted that these hazards may be beyond the control of school, but the following mitigating controls will be implemented:

5.1 Back ups

The school will back up their electronic data and systems every day. This process is managed by Virtual IT Education.

5.2 Fire doors

Areas of the premises which contain paper records or core electronic equipment, such as server boxes, will be fitted with fire doors so that data contained within those areas will be protected, for a period, against any fires that break out on the premises. Fire doors must not be propped open unless automatic door releases are installed.

5.4 Fire alarm system

The school will maintain a fire alarm system at its premises to alert individuals of potential fires and so the necessary fire protocols can be followed.

Systems security

As well as physical security the school also protects against hazards to its IT network and electronic systems. It is recognised that the loss of, or damage to, IT systems could affect the school's ability to operate and could potentially endanger the lives of its students.

The school will implement the following systems security controls to mitigate risks to electronic systems:

6.1 Software download restrictions

Employees are not permitted to download software on to the school's IT systems without permission of Virtual IT Education, who will vet software to confirm its security certificate and ensure the software is not malicious. Virtual IT Education will retain a list of trusted software so that this can be downloaded on to individual desktops without disruption.

6.2 Phishing emails

To avoid the school's computer systems from being compromised through phishing emails employees must not click on links that have been sent to them in emails when the source of that email is unverified.

Employees will also take care when clicking on links from trusted sources in case those email accounts have been compromised.

6.3 Firewalls and anti-virus software

EMCPS will ensure that the firewalls and anti-virus software is installed on electronic devices and routers. The school will update the firewalls and anti-virus

software when updates are made available. The school will review its firewalls and anti-virus software on a regular basis and decide if they are still fit for purpose.

6.5 Shared drives

Upper Wharfedale School maintains a shared drive on its servers and cloud service provider. Whilst employees are encouraged not to store personal and confidential data on the shared drive it is recognised that on occasion there will be a genuine business requirement to do so.

The shared drive will have restricted areas that only authorised employees can access. For example, a HR folder in the shared drive will only be accessible to employees responsible for HR matters. Network Manager will be responsible for giving shared drive access rights to employees.

Communications security

The transmission of personal and confidential data is a key business need and, when operated securely is a benefit to the school and pupils alike. However, data transmission is susceptible to unauthorised and/or malicious loss or corruption. The school has implemented the following transmission security controls to mitigate these risks:

7.1 Sending personal and confidential data by post

When sending personal data, excluding special category data, by post the school will use Royal Mail's standard postal service. Employees will double check addresses before sending and will ensure that the sending envelope does not contain any data which is not intended for the data subject.

7.2 Sending special category data by post

When sending special category data by post the school will use Royal Mail's 1st Class Recorded postal service.

Employees will double check addresses before sending and will ensure that the sending envelope does not contain any data which is not intended for the data subject. If the envelope contains information that is thought to be particularly sensitive, then employees are advised to have the envelope double checked by a colleague.

7.3 Use of email for personal and confidential data

Care must be exercised when sharing information by email. Staff must check that they are sending to the correct address. They should not copy in people who have little need to see the information. Sensitive data should be sent password protected.

When sending emails to many recipients, such as a mail shot, or when it would not be appropriate for recipients to know each other's email addresses then School employees will use the Blind Copy (BCC) function.

Remote working

It is understood that on some occasion employees of the school will need to work at home or away from the school premises. If this is the case, then the employees will adhere to the following controls:

9.1 Lockable storage

If employees are working from home, they will ensure that they have lockable room or storage to keep personal and confidential data and school equipment safe from loss or theft.

Employees must not keep personal and confidential data or school equipment unsupervised at home for extended periods of time (for example when the employee goes on holiday).

Employees must not keep personal and confidential data or school equipment in cars if unsupervised.

9.2 Private working area

Employees must not work with personal and confidential data in areas where other individuals could potentially view it (for example on public transport).

Employees should also take care to ensure that other household members do not have access to personal and confidential data and do not use School equipment for their own personal use.

9.3 Trusted Wi-Fi connections

Employees will only connect their devices to trusted Wi-Fi connections and will not use 'free public Wi-Fi' or 'Guest Wi-Fi' as such connections are susceptible to malicious intrusion.

When using home Wi-Fi networks employees should ensure that they have appropriate anti-virus software and firewalls installed to safeguard against malicious intrusion.

9.4 Encrypted devices and email accounts

Employees will only use school issued encrypted devices to work on personal and confidential data. Employees will not use personal devices for accessing, storing, or creating personal and confidential data. This is because personal devices do not possess the same level of security as a school issued device.

Employees will not use personal email accounts to access or transmit personal and confidential data. Employees must only use school issued, or school authorised, email accounts.

9.5 Data removal and return

Employees will only take personal and confidential data away from the school premises if this is required for a genuine business need.

Employees will take care to limit the amount of data taken away from the premises.

Employees will ensure that all data is returned to the school premises either for re-filing or for safe destruction.

Employees will not destroy data away from the premises as safe destruction cannot be guaranteed.