St Mary's
Catholic Primary School and Nursery

# SCHOOL DATA PROTECTION POLICY

**Legal framework**

This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation (GDPR)
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

This policy will also have regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'
- All Article 29 Working Party Guidance on the implementation of GDPR
- Department of Education 'Data Protection: a toolkit for schools'
- IRMS Information Management Toolkit for Schools.

We implement this Policy in conjunction with the following other school policies:

- Records Management and Retention Policy
- IT Acceptable Use Policy
- Freedom of Information Policy
- Social Media Policy
- Right of Access Policy
- Data Breach Policy
- Security Policy

**Applicable Data**

For the purpose of this Policy:

Personal data refers to information that relates to an identified or identifiable, living individual (Data Subject), including an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

GDPR defines sensitive personal data as 'special categories of personal data'. This includes the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation .

Processing Data means any use of the personal information. This includes collecting, disclosing, destroying, archiving and organising.

The person who the personal data is about is the Data Subject. For example, the children named on a class register at a school are all data subjects of that register.

The Data Controller is usually an organisation who dictates the reason and purpose for how data is processed. The School itself is a Data Controller as it chooses how it collects, uses and shares its own data.

The Information Commissioner's Office (ICO) is the regulator for Data Protection and Privacy law in the UK. They have the power to enforce on organisations for breaches of the Data Protection Act or the GDPR. This means they can issue:

- an undertaking committing an organisation to improving their Data Protection practices
- an Enforcement Notice, ordering an organisation to do something specific e.g. train all staff to a high standard
- a Monetary Penalty for serious and significant breaches. Under the Data Protection Act, this can be anything up to £500,000. Under the General Data Protection Regulation, this can be up to €20 Million or 4% of a company's global turnover

This Policy applies to both automated personal data and to manual filing systems.

**Principles**

In accordance with the requirements outlined in the GDPR, personal data will be:

1. processed fairly, lawfully and transparently
2. processed for a specified and legitimate purpose
3. adequate, relevant and limited to what is relevant
4. accurate and up to date
5. kept no longer than necessary
6. stored securely using technical and organisational measures

The GDPR also requires that "the controller (the school) shall be responsible for, and able to demonstrate, compliance with the principles".

**Accountability**

St Mary's Catholic Primary School & Nursery will implement appropriate technical and organisational measures to demonstrate that we process data in line with the principles set out in the GDPR. This can take a variety of forms. Examples of technical and organisational measures are below:

- **Technical Measures**
    - firewalls
    - anti-virus software
    - encryption
    - secure emails
    - VPNs (Virtual Private Networks)

- **Organisational Measures**
    - policies and procedures in place to help staff understand their duties under data protection
    - training
    - user guides
    - a more knowledgeable and open culture towards Data Protection

St Mary's Catholic Primary School & Nursery will provide comprehensive, clear and transparent privacy notices. We maintain records of activities relating to higher risk processing, such as the processing of special categories data.

In line with best practice, we shall maintain a record of processing activities will include as a minimum the following:

- name and details of the organisation
- purpose(s) of the processing
- description of the categories of individuals and personal data
- retention schedules
- categories of recipients of personal data
- description of technical and organisational security measures

St Mary's Catholic Primary School & Nursery will implement measures that meet the principles of data protection, continuously creating and improving security features.

St Mary's Catholic Primary School & Nursery will produce Data Protection Impact Assessments where the processing of personal data is likely to result in a high risk to the rights of the individual, where a major project requires the processing of personal data or before the introduction of new technology or a significant change to the way, we process data.

**Data Protection Officer (DPO)**

St Mary's Catholic Primary School & Nursery has appointed a DPO to:

- inform and advise St Mary's and its employees about their obligations to comply with the GDPR and other data protection laws
- monitor St Mary's compliance with the GDPR and other laws, including managing internal data protection activities, advising on Data Protection Impact Assessments, conducting internal audits, and providing the required training to staff members.

An experienced and qualified member of staff as designated by Cheshire West and Chester Council will carry out the role of DPO.

St Mary's Catholic Primary School & Nursery will make freely available the contact details for their appointed DPO:

Schools Data Protection Officer
Cheshire West and Chester Council,
Council Offices,
4 Civic Way,
Ellesmere Port,
CH65 0BE

Email: schoolDPO@cheshirewestandchester.gov.uk

The DPO will operate independently, their role being to:

- advise St Mary's about the obligations to comply with GDPR and other data protection requirements – this could be to assist in implementing a new CCTV system or to respond to questions or complaints about information rights
- monitor St Mary's compliance with GDPR, advising on internal data protection activities such as training for staff, the need for data protection impact assessments and conducting internal audits
- act as the first point of contact with the Information Commissioner's Office and for individuals whose data you process

Where advice and guidance offered by the DPO is rejected by St Mary's, this will be independently recorded. However, we will only decline the advice offered by the DPO at the direction of the Governing Body and will be provided to the DPO in writing.

**Lawful Processing**

We will identify the legal basis for processing data and document this prior to data processing data. St Mary's will make it clear, at all times, the basis on which personal data is processed.

We will ensure that we process personal data under one of the following conditions:

- compliance with a legal obligation
- the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- for the performance of a contract with the data subject or to take steps to enter into a contract
- protecting the vital interests of a data subject or another person
- for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject

In addition, we will ensure that we process sensitive data under one of the following conditions:

- explicit consent of the data subject, unless, reliance on consent is prohibited by EU or Member State law
- carrying out obligations under employment, social security or social protection law, or a collective agreement
- protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent

- processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent
- processing relates to personal data manifestly made public by the data subject
- processing is necessary for the establishment, exercise or defence of legal claims
- processing is necessary for reasons of substantial public interest, based on Union or Member state law, with full regard for the rights and interests of the data subject
- processing is necessary for the purposes of preventive or occupational medicine, for example, the assessment of the working capacity of the employee
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

**Consent**

Where there is no other legal basis for the processing of data, St Mary's may rely on the consent of individuals, both parents and pupils, in seeking consent.

Where used, consent must be a positive indication and we cannot infer it from silence, inactivity or pre-ticked boxes. We will only accept consent that is freely given, specific, informed and an unambiguous indication of the individual's wishes. We will keep a record documenting how and when consent was given.

We will review consent previously accepted under the DPA to ensure it meets the standards of the GDPR; however, we will not reobtain acceptable consent obtained under the DPA. The individual can withdraw consent at any time.

We will seek the consent of the parents prior to the processing of a child's data under the age of 13 years except where the processing is preventative or counselling services offered directly to a child.

**The Right to be Informed**

The Privacy Notice supplied to individuals regarding the processing of their personal data will be in clear, plain language that is concise, transparent, easily accessible and free of charge.

If we offer services directly to a child, St Mary's will ensure that the privacy notice is in a clear, plain manner that the child will understand.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, we will supply the following information within the privacy notice:

- the identity and contact details of the controller, and where applicable, the controller's representative and the DPO
- the purpose of, and the legal basis for, processing the data
- any legitimate interests of the controller or third party
- any recipient or categories of recipients of the personal data
- details of transfers to third countries and the safeguards in place
- the retention period of criteria used to determine the retention period
- the existence of the data subject's rights, including the right to:
    - withdraw consent at any time
    - lodge a complaint with a supervisory authority

Where we obtain data directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement and the details of the categories of personal data, as well as any possible consequences of failing to provide the personal data, will be provided.

**The Right of Access**

Individuals have the right to obtain confirmation that their data is being processed.

Individuals also have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing. A form for requesting information is available from the school website www.stmaryscrewe.co.uk

St Mary's will verify the identity of the person making the request before any information is supplied, as well as confirming the subject of the request and the right to make such a request.

We will supply a copy of the information to the individual free of charge; however, we may impose a 'reasonable fee' to comply with requests for further copies of the same information.

Where we receive a SAR electronically, we will provide the information in a commonly used electronic format.

Where a request is manifestly unfounded, excessive or repetitive, we may charge a fee based on administrative cost of providing the information.

We will respond to all requests without delay and at the latest, within one month of receipt.

In the event of numerous or complex requests, the period of compliance will be extended by a further two months. We will inform the individual of the extension and a reason why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. We will inform the individual of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

In the event that we process a large quantity of information about an individual, the school may ask the individual to specify what information the request relates to.

A parent or carer does not have an automatic right to information held about their child. The right belongs to the child and the parent(s) acts on their behalf, where they have parental responsibility for the child. In England, the age at which a child reaches sufficient maturity to exercise their own right to access their information is normally 12, but this may vary amongst individuals. Once a child reaches sufficient maturity, the parent may only act with their child's consent.

Where a child is over 13 years and we receive a request on their behalf, the school may contact them separately to seek their signed consent for someone to access their records on their behalf. When deciding whether the school can release information about a child, consideration will be given to the best interests of the child.

St Mary's will clearly communicate and promote the process for the submission of Subject Access Requests and the exercising of other individual rights as defined under the GDPR during holiday periods, stating clearly how we will handle these requests and how this may impact on any time scales.

**The Right to Rectification**

Individuals are entitled to have any inaccurate or incomplete personal data rectified.

Where appropriate, St Mary's will inform the individual about the information disclosed to third parties. Where the personal data in question has been disclosed to third parties, St Mary's will inform the third party of the rectification where possible.

Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

Where we will not take action in response to a request for rectification, St Mary's will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

**The Right to Erasure**

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

The right to erasure is not absolute. Individuals have the right to erasure in the following circumstances:

- where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- when the individual withdraws their consent
- when the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- the personal data was unlawfully processed
- the personal data is required to be erased in order to comply with a legal obligation

St Mary's has the right to refuse a request for erasure where we process the personal data for the following reasons:

- to exercise the right of freedom of expression and information
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority
- for public health purposes in the public interest
- for archiving purposes in the public interest, scientific research, historical research or statistical purposes
- the exercise or defence of legal claims

As a child may not fully understand the risks involved in the processing of data when we obtain consent: we therefore give special attention to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

Where we disclose personal data to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Where personal data has been made public within an online environment, St Mary's will inform other organisations who process the personal data to erase links to and copies of the personal data in question where possible.

**The Right to Restrict Processing**

Individuals have the right to block or suppress the school's processing of personal data. In the event that processing is restricted, St Mary's will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

St Mary's will restrict the processing of personal data in the following circumstances:

- where an individual contests the accuracy of the personal data, processing will be restricted until St Mary's has verified the accuracy of the data
- where an individual has objected to the processing and St Mary's is considering whether their legitimate grounds override those of the individual
- where processing is unlawful and the individual opposes erasure and requests restriction instead
- where St Mary's no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

If the personal data in question has been disclosed to third parties, St Mary's will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

St Mary's will inform individuals when a restriction on processing has been lifted.

**The Right to Data Portability**

Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

Personal data can be easily moved, copied or transferred from one IT environment to another and this can be completed in a safe and secure manner, without hindrance to usability.

The right to data portability only applies in the following cases:

- to personal data that an individual has provided to a the school
- where the processing is based on the individual's consent or for the performance of a contract
- when processing is carried out by automated means

Personal data will be provided in a structured, commonly used and machine-readable form and free of charge.

Where feasible, we will transfer data directly to another organisation at the request of the individual. However, we are not obligated to adopt or maintain processing systems that are technically compatible with other organisations.

In the event that the personal data concerns more than one individual, St Mary's will consider whether providing the information would prejudice the rights of any other individual.

St Mary's will respond to any requests for portability within one month. We can extend the timeframe by two months where the request is complex or we receive a number of requests. If this is the case, we will inform the individual of the extension and the reasoning behind it within one month of the receipt of the request.

Where no action is being taken in response to a request, St Mary's will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

**The Right to Object**

St Mary's will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

Individuals have the right to object to the following:

- processing based on legitimate interests or the performance of a task in the public interest
- direct marketing undertaken by or on behalf of the school
- processing for purposes of scientific or historical research and statistics

The performance of a legal task or legitimate interests:

- an individual's grounds for objecting must relate to his or her particular situation
- St Mary's will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual

Direct marketing purposes:

- St Mary's will stop processing personal data for direct marketing purposes as soon as we receive an objection

- St Mary's cannot refuse an individual's objection regarding data processed for direct marketing purposes

Research purposes:

- the individual must have grounds relating to their particular situation in order to exercise their right to object
- where the processing of personal data is necessary for the performance of a public interest task, St Mary's is not required to comply with an objection to the processing of the data.

Where the processing activity outlined above, is carried out online, St Mary's will offer a method for individuals to object online.

**Privacy by Design and Data Protection Impact Assessments**

St Mary's will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the school has considered and integrated data protection into processing activities.

We use Data Protection Impact Assessments (DPIAs) to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy. This will allow us to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage to our reputation that might otherwise occur.

We will use a DPIA for new technologies, or when processing is likely to result in a high risk to the individuals' rights and freedoms. We may also use a DPIA for more than one project, or where the aims and conditions of the projects are the same.

St Mary's will ensure that all DPIAs include the following information:

- a description of the processing operations and the purposes
- an assessment of the necessity and proportionality of the processing in relation to the purpose
- an outline of the risks to individuals
- the measures implemented in order to address risk

Where a DPIA indicates high-risk data processing, we will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

**Data Processors**

St Mary's will ensure that whenever it employs or utilises a data processor a written contract will be in place. Any contract will include, as a minimum, specific terms under which we allow processing and will document:

- only act on the written instructions of the controller
- ensure that people processing the data are subject to a duty of confidence
- take appropriate measures to ensure the security of processing
- only engage sub-processors with the prior consent of the controller and under a written contract
- assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR
- assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments
- delete or return all personal data to the controller as requested at the end of the contract
- submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state

Where appropriate, and when supplied by the Information Commissioner's Office, we will supplement standard clauses.

Any contract will clearly identify the responsibilities and liabilities of data processors regarding:

- not using a sub-processor without the prior written authorisation of the data controller
- the co-operation with supervisory authorities (such as the ICO)
- the security of its processing
- the record keeping of processing activities
- the notification of any personal data breaches to the data controller
- the employment of a Data Protection Officer
- the appointment (in writing) of a representative within the European Union if needed

Where a processor fails in these obligations or acts outside of the direct instructions of the school, appropriate action will be taken.

**Data Breaches**

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

St Mary's will ensure that all staff are aware of, and understand, what constitutes a data breach as part of their continuous development training.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

Our Data Protection Officer will report all notifiable breaches to the relevant supervisory authority, within 72 hours of being aware of it.

We will assess the risk of the breach having a detrimental effect on the individual and the need to notify the relevant supervisory authority on a case-by-case basis. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, St Mary's will notify those concerned directly.

A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority. In the event that a breach is sufficiently serious, we will notify the public without undue delay.

Effective and robust breach detection, investigation and internal reporting procedures are in place at St Mary's. These facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

We will outline the following information within a breach notification:

- the nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- the name and contact details of the DPO
- an explanation of the likely consequences of the personal data breach
- a description of the proposed measures to be taken to deal with the personal data breach
- where appropriate, a description of the measures taken to mitigate any possible adverse effects

Failure to report a breach when required to do so will be a breach of school policy and an additional breach of the GDPR.

**Data Security**

St Mary's will keep confidential paper records in a locked filing cabinet or cupboard with restricted access.

We will not leave confidential paper records unattended, or in clear view anywhere with general access.

Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

Where we save data on removable storage or a portable device, it will be kept in a locked filing cabinet, drawer or safe when not in use.

We will not store personal information on memory sticks unless they are password-protected and fully encrypted.

All electronic devices are password-protected to protect the information on the device in case of theft.

Where possible, St Mary's enables electronic devices to allow the remote blocking or deletion of data in case of theft.

Staff and governors will not use their personal laptops or computers for school purposes.

We provide all necessary members of staff with their own secure login and password, and computers regularly prompts users to change their password.

Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

We send circular emails to parents' blind carbon copy (bcc), to ensure we do not disclose email addresses to other recipients.

When we take personal information, considered private or confidential, off the premises in an electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.

Before sharing data, all staff members will ensure:

- they are allowed to share it
- that adequate security is in place to protect it

- who will receive the data has been outlined in a privacy notice

Under no circumstances will we allow access to confidential or personal information. We will supervise visitors at all times, in areas of St Mary's that contain sensitive information.

The physical security our buildings and storage systems, and access to them, is reviewed on an annual basis. If we identify an increased risk in vandalism/burglary/theft, we will put extra measures in place to secure data storage.

Any unauthorised disclosure or personal or sensitive information may result in disciplinary action.

**Publication of Information**

St Mary's will not publish any personal information, including photos, on its website, in social media or in any promotional or marketing publication without the permission of the affected individual.

When uploading information to the school website, staff are considerate of any metadata or deletions, which could be accessed in documents and images on the site.

**Data Retention**

We will not keep data for longer than is necessary in line with the schools Record Management Policy and we will delete any unrequired data as soon as practicable.

We will keep some educational records relating to former pupils or employees of St Mary's for an extended period for legal reasons, or to enable the provision of references or academic transcripts.

Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed.

**DBS Data**

We will handle all data provided by the DBS in line with data protection legislation; this includes electronic communication.

We will never duplicate data provided by the DBS.

We will make any third parties who access DBS information aware of the data protection legislation, as well as their responsibilities as a data handler.