

St Mary's Catholic Primary School

DATA PROTECTION POLICY

DATE OF APPROVAL	14/01/19
VERSION DATE	V.01
DATE UPLOADED	
DATE FOR REVIEW	05/2020
OWNER	F&R Committee

Contents

1. Aims2

2. Legislation and guidance2

3. Data protection principles.....2

4. Definitions.....2

5. The data controller3

6. Roles and responsibilities3

7. Collecting personal data.....4

8. Sharing personal data4

9. Subject access requests and other rights of individuals5

10. Parental requests to see the educational record6

11. Photographs and videos6

12. Data protection by design and default7

13. Data security and storage of records7

14. Disposal of records7

15. Personal data breaches8

16. Training8

17. Monitoring arrangements8

Appendix 1: Personal data breach procedure.....9

RELATED SCHOOL POLICIES AND DOCUMENTS

- E-Safety Policy
- Data Protection Impact Assessment Policy & Procedure
- Subject Access Request Policy & Procedure
- Information Security Incident Procedure
- Records Retention Procedure
- Freedom of Information Policy

1. Aims

St Mary's 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 \(GDPR\)](#) 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.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. 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](#).

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.

3. Data protection principles

GDPR is based on data protection principles that our school must comply with. The principles say that personal data must be:

- 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.

4. Definitions

Term	Definition
Personal data	<p>Any information relating to an identified, or identifiable, individual.</p> <p>This may include the individual's:</p> <ul style="list-style-type: none">• Name (including initials)• Identification number• Location data• Online identifier, such as a username <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</p>
Special categories of personal data	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none">• Racial or ethnic origin• Political opinions• Religious or philosophical beliefs• Trade union membership• Genetics• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes

	<ul style="list-style-type: none"> • Health – physical or mental • Sex life or sexual orientation
Processing	<p>Anything done to personal data, such as collecting, recording, organizing, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.</p> <p>Processing can be automated or manual.</p>
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

The School processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The School is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

6. Roles and responsibilities

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

6.1 Governing Body

The Governing Body has overall responsibility for ensuring that the School complies with all relevant data protection obligations.

6.2 Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law, and developing related policies and guidelines where applicable.

The DPO 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 Headteacher as the Deputy Data Protection Officer (DDPO) acts as the representative of the data controller on a day-to-day basis.

The Data Protection Officer (DPO) for St Mary's School is Integra Limited.

The Deputy Data Protection Officer (DDPO) for St Mary's School is the Headteacher, Mrs Jane Howie-Lee

The Governing Body Link governor for GDPR and Data Protection issues is Mr Brian Wheelwright.

The DPO is also the first point of contact for individuals whose data the School processes, and for the ICO. Full details of the DPO's responsibilities are set out in the School's contract with the company.

6.3 All staff

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 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 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. Collecting personal data

7.1 Lawfulness, fairness and transparency

The School will only process personal data where it has one of 6 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, the School will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

Where the School offers online services to pupils, such as classroom apps, and it intends to rely on consent as a basis for processing, the School will get parental consent (except for online counselling and preventive services).

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

7.2 Limitation, minimisation and accuracy

The School will only collect personal data for specified, explicit and legitimate reasons. It will explain these reasons to the individuals when we first collect their data.

If the School wants to use personal data for reasons other than those given when it is first obtained, it will inform the individuals concerned before it does so and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymized. This will be done in accordance with the [Information and Records Management Society's toolkit for schools](#).

8. Sharing personal data

The School will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of staff at risk

- It needs to liaise with other agencies – it will seek consent as necessary before doing this
- Suppliers or contractors need data to enable the School to provide services to staff and pupils; for example, IT companies. When doing this, the School will:
 - Only appoint suppliers or contractors that 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 shared
 - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with the School

The School will also share personal data with law enforcement and government bodies where legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided

The School may also share personal data with emergency services and local authorities to help them to respond to an emergency that affects pupils or staff.

Where the School transfers personal data to a country or territory outside the European Economic Area, it will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 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
- 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

Subject access requests must be submitted in writing, either by letter, email or fax to the DPO via the DDPO. They should include:

- 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 DDPO.

9.2 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 the School may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, the School:

- May ask the individual to provide 2 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
- Will provide the information free of charge
- 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

The School will not disclose information 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
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, the School may refuse to act on it, or charge a reasonable fee which considers administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When a request is refused, the School will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 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 the School is collecting their data about how it will 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, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified based on public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- 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 via the DDPO. If staff receive such a request, they must immediately forward it to the DDPO.

10. Parental requests to see the educational 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.

11. Photographs and videos

As part of the School's activities, photographs and record images may be made of individuals within the School. The School will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. The School will explain clearly how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within school on display boards and in school prospectus

- Outside of school by external agencies such as the School photographer, newspapers, special events
- Online on the School website or social media pages

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

When using photographs and videos in this way the School will not accompany them with any other personal information about the child, to ensure they cannot be identified.

The School E-Safety Policy contains a Responsible Internet Use Consent Form and more information on the School's use of photographs and videos.

12. Data protection by design and default

The School will put measures in place to show that it has integrated data protection into its 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
- 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; the School will also keep a record of attendance
- Regularly conducting reviews and audits to test privacy measures and ensure that the School is compliant
- Maintaining records of the School's processing activities, including:
 - For the benefit of data subjects, making available the name and contact details of the School and DPO and all information it is required to share about how it uses and process their personal data (via our privacy notices)
 - For all personal data that it holds, maintaining an internal record of the type of data, data subject, how and why it is using the data, any third-party recipients, how and why it is storing the data, retention periods and how it is keeping the data secure

13. Data security and storage of records

The School 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 staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the School Office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. 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, pupils or 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).
- Where the School needs to share personal data with a third party, it will carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

14. 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 it cannot be rectified or updated. For example, the School will shred paper-based records, and overwrite or delete electronic files. It may also use a third party to dispose of records safely on the School's behalf. Where this is done, the third party will be required to provide guarantees that it complies with data protection law.

15. 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, the School will follow the procedure set out in Appendix 1.

When appropriate, the School will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymized dataset being published on the School website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

16. 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.

17. Monitoring arrangements

The Governing Body in conjunction with the DP and DDPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated every two years and shared with the full governing board. The two-year review frequency reflects the information in the [Department for Education's advice on statutory policies](#).

Appendix 1: Personal data breach procedure

This procedure is based on [guidance on personal data breaches](#) produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DDPO
- The DDPO will investigate the report and determine whether a breach has occurred. The DPO will consider whether personal data has been accidentally or unlawfully:
 - Lost
 - Stolen
 - Destroyed
 - Altered
 - Disclosed or made available where it should not have been
 - Made available to unauthorised people
- The DDPO will alert the DPO and the Chairman of Governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will evaluate whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. The DPO will consider whether the breach is likely to affect people's rights and freedoms negatively, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
 - Loss of control over their data
 - Discrimination
 - Identify theft or fraud
 - Financial loss
 - Unauthorised reversal of pseudonymisation (for example, key-coding)
 - Damage to reputation
 - Loss of confidentiality
 - Any other significant economic or social disadvantage to the individual(s) concerned
- The DPO and DDPO will document the decision if it is challenged later by the ICO or an individual affected by the breach. Documented decisions are stored on the School's computer system.
- Where the ICO must be notified, the DPO will do this via the ['report a breach' page of the ICO website](#) within 72 hours. As required, the DPO will set out:
 - A description of the nature of the personal data breach including, where possible:
 - The categories and approximate number of individuals concerned
 - The categories and approximate number of personal data records concerned
 - The name and contact details of the DPO
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
 - The name and contact details of the DPO
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. Records of all breaches will be stored on the school's computer system. For each breach, this record will include the:
 - Facts and cause
 - Effects
 - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error. Types of breach might include details of pupil premium interventions for named children, or non-anonymised pupil exam results or staff pay information being shared with governors.
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask a member of the admin team to do so
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted