

Saint Mary's Catholic Primary School



DATA PROTECTION POLICY

1. Rationale

St Mary's School is committed to a policy of protecting the rights and privacy of individuals, including pupils, staff and others, in accordance with the Data Protection Act, 1998 (DPA).

St Mary's School needs to process certain information about its staff, pupils and other individuals with whom it has a relationship for various purposes such as, but not limited to:

- the recruitment and payment of staff
- the administration of programmes of study
- the recording of a student's progress
- agreeing awards
- collecting fees
- complying with legal obligations to funding bodies and government

To comply with various legal obligations, including the obligations imposed on it by the Data Protection Act, 1998, St Mary's School must ensure that all this information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully.

2. Compliance

This policy applies to all governors, staff and pupils of St Mary's School. Any breach of this policy, or of the Act itself will be considered an offence and St Mary's School's disciplinary procedures will be invoked.

As a matter of best practice, other agencies and individuals working with St Mary's School, and who have access to personal information, will be expected to read and comply with this policy. It is expected that departments or individuals who are responsible for dealing with external bodies will take the responsibility for ensuring that such bodies sign a contract which among other things will include an agreement to abide by this policy.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the DPA and other relevant legislation.

The Information Commissioner's Office (ICO) <https://ico.org.uk/> gives further detailed guidance and St Mary's School undertakes to adopt and comply with ICO guidance.

3. The Data Protection Act, 1998

This piece of legislation came into force on 1 March 2000. The DPA regulates the processing of personal data, and protects the rights and privacy of all living individuals (including children), for example by giving all individuals who are the subject of personal data a general right of access to the personal data which relates to them. Individuals can exercise the right to gain access to their information by means of a 'subject access request' (sample held at Appendix A). Personal data is information relating to an individual and may be in hard or soft copy (paper/ manual files; electronic records; photographs; CCTV images), and may include facts or opinions about a person.

The DPA also sets out specific rights for school pupils in relation to educational records held within the state education system. These rights are set out in separate education regulations 'The Education (Student Information) (England) Regulations 2000.' For more detailed information on these Regulations see the Data Protection Guide on the ICO website.

4. Responsibilities Under the DPA and Registration

St Mary's School will be the 'data controller' under the terms of the legislation – this means it is ultimately responsible for controlling the use and processing of the personal data.

The Head teacher of St Mary's School is responsible for all day-to-day data protection matters, and she will be responsible for ensuring that all members of staff and relevant individuals abide by this policy, and for developing and encouraging good information handling within St Mary's School.

St Mary's School is registered as a Data Controller on the Data Protection Register held by the Information Commissioner. Current registration reference: Z8171429

The Head teacher is also responsible for ensuring that St Mary's School's notification is kept accurate. Details of St Mary's School's notification can be found on the ICO website.

Compliance with the legislation is the responsibility of all members of St Mary's School who process personal information.

Individuals who provide personal data to St Mary's School are responsible for ensuring that the information is accurate and up-to-date.

5. Data Protection Principles

The legislation places a responsibility on every data controller to process any personal data in accordance with the eight principles. In order to comply with its obligations, St Mary's School undertakes to:

5.1 Process personal data fairly and lawfully

St Mary's School will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller; the purposes of the processing; any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant.

5.2 Process the data for the specific and lawful purpose for which it collected that data, and not further process the data in a manner incompatible with this purpose

St Mary's School will ensure that the reason for which it collected the data originally is the only reason for which it processes those data, unless the individual is informed of any additional processing before it takes place.

5.3 Ensure that the data is adequate, relevant and not excessive in relation to the purpose for which it is processed

St Mary's School will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this in mind. If any irrelevant data are given by individuals, they will be destroyed immediately.

5.4 Keep personal data accurate and, where necessary, up to date

St Mary's School will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify St Mary's School if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of St Mary's School to ensure that any notification regarding the change is noted and acted on.

5.5 Only keep personal data for as long as is necessary

St Mary's School undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. This means St Mary's School will undertake a regular review of the information held and implement a weeding process when, e.g. pupils or a member of staff leaves St Mary's School.

St Mary's School will dispose of any personal data in a way that protects the rights and privacy of the individual concerned. See also Section 16.

5.6 Process personal data in accordance with the rights of the data subject under the legislation

Individuals have various rights under the legislation including:

- a right to be told the nature of the information St Mary's School holds and any parties to whom this may be disclosed;
- a right to prevent processing likely to cause damage or distress;
- a right to prevent processing for purposes of direct marketing;
- a right to be informed about the mechanics of any automated decision making process that will significantly affect them;
- a right not to have significant decisions that will affect them taken solely by automated process;
- a right to sue for compensation if they suffer damage by any contravention of the legislation;

- a right to take action to rectify, block, erase, or destroy inaccurate data;
- a right to request that the Office of the Information Commissioner assess whether any provision of the Act has been contravened;

St Mary's School will only process personal data in accordance with individuals' rights.

5.7 Put appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data

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

St Mary's School will ensure that all personal data is accessible only to those who have a valid reason for using it.

St Mary's School will have in place appropriate security measures e.g.

- ensuring that hard copy personal data is kept in lockable filing cabinets/ cupboards with controlled access;
- keeping all personal data in a lockable room with key-controlled access;
- password protecting personal data held electronically;
- archiving personal data on disks which are then kept securely (lockable cabinet);
- placing any PCs or terminals, CCTV camera screens etc. that show personal data so that they are not be visible except to authorised staff.

In addition, St Mary's School will put in place appropriate measures for the deletion of personal data – manual records will be shredded or disposed of as 'confidential waste', and appropriate contract terms will be put in place with any third parties undertaking this work. Hard drives of redundant PCs will be wiped clean before disposal, or if that is not possible, destroyed physically.

This policy also applies to staff and pupils who process personal data 'off-site', e.g. when working at home, and in such circumstances additional care must be taken regarding the security of the data.

5.8 Ensure that no personal data is transferred to a country or a territory outside the European Economic Area unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

St Mary's School will not transfer data to such territories without the explicit consent of the individual.

This also applies to publishing information on the Internet – because transfer of data can include placing data on a website that can be accessed from outside the EEA – so St Mary's School will always seek the consent of individuals before placing any personal data (including photographs) on its website.

If St Mary's School collects personal data in any form via its website, it will provide a clear and detailed privacy statement prominently on the website, and wherever else personal data is collected.

6. Consent as a Basis for Processing

Although it is not always necessary to gain consent from individuals before processing their data, it is often the best way to ensure that data is collected and processed in an open and transparent manner.

Consent is especially important when schools are processing any sensitive data, as defined by the legislation.

St Mary's School understands consent to mean that the individual has been fully informed of the intended processing and has signified their agreement (e.g. via signing a form), whilst being of a sound mind and without having any undue influence exerted upon them. Consent obtained on the basis of misleading information will not be a valid basis for processing. Consent cannot be inferred from the non-response to a communication.

St Mary's School will ensure that any forms used to gather data on an individual will contain a statement (Privacy Notice – formerly known as Fair Processing Notice) explaining the use of that data, how the data may be disclosed, and also indicate whether or not the individual needs to consent to the processing.

St Mary's School will ensure that if the individual does not give her consent for the processing, and there is no other lawful basis on which to process the data, then steps will be taken to ensure that processing of that data does not take place.

7. Subject Access Rights (SARS)

The Data Protection Acts extend to all data subjects a right of access to their own personal data. In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place. Where a request for subject access is received from a pupil, St Mary's School's policy is that:

- Requests from pupils will be processed as any subject access request as outlined below and the copy will be given directly to the pupil, unless it is clear that the pupil does not understand the nature of the request.
- Requests from pupils who do not appear to understand the nature of the request will be referred to their parents or carers.
- Requests from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent.

7.1 Processing Subject Access Requests

Requests for access must be made in writing.

8. Authorised Disclosures

St Mary's School will, in general, only disclose data about individuals with their consent. However there are circumstances under which St Mary's School's authorised officer may need to disclose data without explicit consent for that occasion.

These circumstances are strictly limited to:

- Pupil data disclosed to authorised recipients related to education and administration necessary for St Mary's School to perform its statutory duties and obligations.
- Pupil data disclosed to authorised recipients in respect of their child's health, safety and welfare.
- Pupil data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of St Mary's School.
- Staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters.
- Unavoidable disclosures, for example to an engineer during maintenance of the computer system. In such circumstances the engineer would be required to sign a form promising not to disclose the data outside St Mary's School. Officers and IT personnel writing on behalf of the LA are IT liaison/data processing officers, for example in the LA, are contractually bound not to disclose personal data.
- Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within St Mary's School by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within St Mary's School who **need to know** the information in order to do their work. St Mary's School will not disclose anything on pupils' records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything where suggests that they are, or have been, either the subject of or at risk of child abuse.

8.1 Legal Disclosure

A **"legal disclosure"** is the release of personal information from the computer to someone who requires the information to do his or her job within or for St Mary's School, provided that the purpose of that information has been registered.

8.2 Illegal Disclosure

An **"illegal disclosure"** is the release of information to someone who does not need it, or has no right to it, or one which falls outside St Mary's School's registered purposes.

9. Publication of School Information

St Mary's School publishes various items which will include some personal data, e.g.

- internal telephone directory
- event information

- staff information
- lists of pupils

It may be that in some circumstances an individual wishes their data processed for such reasons to be kept confidential, or restricted to internal school access only. Therefore it is School policy to offer an opportunity to opt-out of the publication of such when collecting the information.

Staff records appertaining to individual staff will remain of a confidential nature between the Head teacher and the member of staff and, where appropriate, St Mary's School HR Manager.

9.1 Email

It is the policy of St Mary's School to ensure that senders and recipients of email are made aware that under the DPA, and Freedom of Information legislation, the contents of email may have to be disclosed in response to a request for information. One means by which this will be communicated will be by a disclaimer on St Mary's School's email.

Under the Regulation of Investigatory Powers Act 2000, Lawful Business Practice Regulations, any email sent to or from St Mary's School may be accessed by someone other than the recipient for system management and security purposes.

9.2 CCTV

There are CCTV systems operating within St Mary's School for the purpose of protecting school members and property. St Mary's School will only process any personal data obtained by the CCTV system in a manner which ensures compliance with the legislation.

For detailed guidance on CCTV refer to the ICO 'In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Data, May 2015 which can be found at <https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf> and St Mary's School CCTV Procedures appended to this Policy.

10. Data Integrity

St Mary's School undertakes to ensure data integrity by the following methods:

10.1 Data Accuracy

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs St Mary's School of a change of circumstances their computer record will be updated as soon as is practicable. A printout of their data record will be provided to data subjects every twelve months so they can check its accuracy and make any amendments.

Where a data subject challenges the accuracy of their data, St Mary's School will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Governing Body for their judgement. If the problem cannot be resolved at this stage, either side may seek independent arbitration. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

10.2 Data Adequacy and Relevance

Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. In order to ensure compliance with this principle, St Mary's School will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data. Data held about individuals will not be kept for longer than necessary for the purposes registered. In order to ensure compliance with this principle, the senior Administrator will check records annually on completion of the annual update form, for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data. The School Administrator using the data provided by parents has the authority to delete as necessary.

10.3 Length of Time

Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of the Senior Administrator and Headteacher to ensure that obsolete data are properly erased. See also Section 16.

11. Data and Computer Security

St Mary's School undertakes to ensure security of personal data by the following general methods (precise details cannot, of course, be revealed):

11.1 Physical Security

Appropriate building security measures are in place, such as alarms, door code locks, deadlocks and computer hardware cable locks. Only authorised persons are allowed in the computer room. Disks, tapes and printouts are locked away securely when not in use. Visitors to St Mary's School are required to sign in and out, to wear identification badges whilst in St Mary's School and are, where appropriate, accompanied.

11.2 Logical Security

- Security software is installed on all computers containing personal data.
- St Mary's School will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them.
- All users will be given secure user names and strong passwords which must be changed regularly. User names and passwords must never be shared.
- St Mary's subscribes to the CICT school's IT services from May 2017. This provides service for school to get Internet content filtering, Sophos Antivirus and managed email hosting (based on Office 365)
- Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.
- All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.
- Personal data can only be stored on school equipment where allowed. Private equipment (i.e. owned by the users) must not be used.
- When personal data is stored on any portable computer system, USB stick or any other removable media:
 - the data must be encrypted and password protected;
 - the device must be password protected (many memory sticks/cards and other mobile devices cannot be password protected);
 - the device must offer approved virus and malware checking software;
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.
- St Mary's School do not allow storage of personal data on removable devices.
- St Mary's School has clear procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups. The school benefits from a simple server to control user access and provide central storage of files. Security is configured by logins or groups of logins to allow access to various data. By storing data centrally this allows us to manage an effective backup solution
- Cloud backups, also offer a subscription for backups so that we don't need to rotate or take disk offsite manually.

11.3 Procedural Security

In order to be given authorised access to the computer, staff will have to undergo checks and will sign a confidentiality agreement. All staff are trained in their Data Protection obligations and their knowledge updated as necessary. Computer printouts as well as source documents are shredded before disposal.

Further information can be found in St Mary's School Online Safety Policy.

Overall security policy for data is determined by Eddie Byrne, Governing Body, and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent. St Mary's School's security policy is kept in a safe place at all times.

Any queries or concerns about security of data in St Mary's School should in the first instance be referred to Eddie Byrne, Governing Body.

Individual members of staff can be personally liable in law under the terms of the Data Protection Acts. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as disciplinary matter, and serious breaches could lead to dismissal.

12. Secure transfer of data and access out of school

St Mary's School recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or personal data from St Mary's School or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school.
- When data is required by an authorised user from outside St Mary's School premises (for example, by a teacher or student working from their home or a contractor) they must have secure remote access to the management information system (MIS) or learning platform.
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority in this event. (NB. to carry encrypted material is illegal in some countries)

13. Disposal of Data

St Mary's School will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of protected data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten and other media must be shredded, incinerated or otherwise disintegrated for data.

A Destruction Log will be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

14. Training & Awareness

All staff will receive data handling awareness/data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff;
- Staff meetings/briefings/Inset;
- Day to day support and guidance from the Headteacher or designated safeguard lead.

15. Enquiries

Information about St Mary's School's Data Protection Policy is available from Mrs Julie Dyer, *Senior Administrator*. General information about the Data Protection Act can be obtained from the Information Commissioners Office <https://ico.org.uk/>.

A copy of this policy will be available to all employees and covered in new staff Induction Training. It will be reviewed at least biennially, added to, or modified from time to time and may be supplemented in appropriate cases by further statements and procedures relating to the work of the particular groups of workers.

Signed: Executive Headteacher: *S.L. Slack*

Signed: Chair of Governors: *G. Duncan*

Date: Updated September 2020

ACCESS TO PERSONAL DATA REQUEST
(Subject Access Request – SARS)

DATA PROTECTION ACT 1998 (Section 7)

Enquirer's Surname		Enquirer's Forenames	
Enquirer's Address			
Enquirer's Postcode:			
Enquirer's Tel No.			
Are you the person who is the subject of the records you are enquiring about (i.e. the "Data Subject")?			YES / NO
If NO,			
Do you have parental responsibility for a child who is the "Data Subject" of the records you are enquiring about?			YES / NO
If YES,			
Name of child or children about whose personal data records you are enquiring:	<hr/> <hr/> <hr/> <hr/>		
Description of Concern / Area of Concern			
Description of Information or Topic(s) Requested (In your own words)			
Additional Information			

Please despatch Reply to: *(if different from enquirer's details as stated on this form)*

Name

Address

Postcode

DATA SUBJECT DECLARATION

I request that St Mary's School search its records based on the information supplied above under Section 7 (1) of the Data Protection Act 1998 and provide a description of the personal data found from the information described in the details outlined above relating to me (or my child/children) being processed by St Mary's School.

I agree that the reply period will commence when I have supplied sufficient information to enable St Mary's School to perform the search.

I consent to the reply being disclosed and sent to me at my stated address (or to the Despatch Name and Address above who I have authorised to receive such information).

Signature of "Data Subject" (or Subject's Parent) _____

Name of "Data Subject" (or Subject's Parent) (PRINTED) _____

Dated _____

Privacy Notices:

St Mary's School workforce: those employed to teach, or otherwise engaged to work at, a school or a local authority

The Data Protection Act 1998: How we use your information

We process personal data relating to those we employ to work at, or otherwise engage to work at our school/local authority. This is for employment purposes to assist in the running of St Mary's School/authority and/or to enable individuals to be paid. The collection of this information will benefit both national and local users by:

- improving the management of workforce data across the sector
- enabling development of a comprehensive picture of the workforce and how it is deployed
- informing the development of recruitment and retention policies
- allowing better financial modelling and planning
- enabling ethnicity and disability monitoring; and
- supporting the work of St Mary's School Teachers' Review Body

This personal data includes identifiers such as names and National Insurance numbers and characteristics such as ethnic group, employment contracts and remuneration details, qualifications and absence information.

We will not share information about you with third parties without your consent unless the law allows us to. We are required, by law, to pass on some of this personal data to:

- our local authority
- the Department for Education (DfE)

If you require more information about how we and/or DfE store and use your personal data please visit:

- our local authority at <http://www.cumbria.gov.uk/childrensservices/schoolsandlearning/schools/privacynotice.asp>; or
- <https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

If you want to see a copy of information about you that we hold, please contact:

Children's Services Tel: 01228 221271 email: ros.dean@cumbria.gov.uk
 website: www.cumbria.gov.uk/childrensservices

THIS PAGE IS INTENTIONALLY BLANK FOR PRINTING PURPOSES

Privacy Notices:

Information about pupils in schools, alternative provision, pupil referral units and children in early years settings

Data Protection Act 1998: How we use pupil information

We collect and hold personal information relating to our pupils and may also receive information about them from their previous school, local authority and/or the Department for Education (DfE). We use this personal data to:

- support our pupils' learning
- monitor and report on their progress
- provide appropriate pastoral care; and
- assess the quality of our services

This information will include their contact details, national curriculum assessment results, attendance information, any exclusion information, where they go after they leave us and personal characteristics such as their ethnic group, any special educational needs they may have as well as relevant medical information. *For pupils enrolling for post 14 qualifications, the Learning Records Service will give us the unique learner number (ULN) and may also give us details about your learning or qualifications.*

We will not give information about our pupils to anyone without your consent unless the law and our policies allow us to do so. If you want to receive a copy of the information about your son/daughter that we hold, please contact:

- Mrs Julie Dyer, school administrator

We are required, by law, to pass certain information about our pupils to our local authority (LA) and the Department for Education (DfE).

We are required, by law, to pass some information about our pupils to the Department for Education (DfE). This information will, in turn, then be made available for use by the LA.

DfE may also share pupil level personal data that we supply to them, with third parties. This will only take place where legislation allows it to do so and it is in compliance with the Data Protection Act 1998.

Decisions on whether DfE releases this personal data to third parties are subject to a robust approval process and are based on a detailed assessment of who is requesting the data, the purpose for which it is required, the level and sensitivity of data requested and the arrangements in place to store and handle the data. To be granted access to pupil level data, requestors must comply with strict terms and conditions covering the confidentiality and handling of data, security arrangements and retention and use of the data.

For more information on how this sharing process works, please visit: <https://www.gov.uk/guidance/national-pupil-database-apply-for-a-data-extract>

For information on which third party organisations (and for which project) pupil level data has been provided to, please visit: <https://www.gov.uk/government/publications/national-pupil-database-requests-received>

If you need more information about how our local authority and/or DfE collect and use your information, please visit:

- our local authority at <http://www.cumbria.gov.uk/childrensservices/schoolsandlearning/schools/privacynotice.asp>; or
- the DfE website at <https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>