St Mary's CE Primary School

Data Protection Policy

1. Rationale

The Data Protection Act 1998 is the law that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's personal data.

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the Data Protection Act. It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

2. Scope of the Policy

Personal information is any information that relates to a living individual who can be identified from the information. This includes any expression of opinion about an individual and intentions towards an individual. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings.

At our School we acknowledge that to function properly we need to collect and use certain types of information about staff, students and other individuals who come into contact with school. We are also obliged to collect and use data to fulfil our obligations to the Local Authority, Department for Education and other bodies. We deal with all information properly in whatever way it is collected, recorded and used – on paper, in a computer, or recorded on other material. We regard the lawful and correct treatment of personal information as very important to successful operations, and to maintaining confidence between those with whom we deal and ourselves. We ensure that our organisation treats personal information lawfully and correctly. To this end we fully endorse and adhere to the Principles of Data Protection, as detailed in the Data Protection Act 1998.

The Governing Body of the school has overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions.
The Headteacher and Governors of this School intend to comply fully with the requirements and principles of the Data Protection Act 2018. All staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities within these guidelines.

There are changes to be made with the advent of the General Data Protection Regulation which becomes law on 25th May 2018 of which the school is aware and is working towards compliance.

3. Data Protection Principles

The Act is based on eight data protection principles, or rules for 'good information handling'.

All members of staff employed in our school are required to adhere to the eight data protection principles set out in the 1998 Data Protection Act:

1. Data shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met.
   Under GDPR, conducting criminal record checks on employees must be justified by law.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Genetic and biometric information is now considered sensitive data, meaning that organisations may only request such information if it is required for a relevant purpose.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Privacy notices or "how we use your information" guides now need to be clearer than before. This means that mere consent is not enough; the individual must be informed of exactly what their data is being used for. Further, organisations must inform the person of their right to withdraw consent at any time.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under the Act.

A new "right to be forgotten" in the GDPR means that someone can request that online content is removed from an organisation's database. ***The Data Portability Act*** *means that a person can request all their personal data be transferred to another system for free.*

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Companies are now required to appoint a Data Protection Officer, or DPO. The DPO is responsible for everything related to keeping personal data secure and cannot be easily replaced. Appointing someone in this position means personal data can be kept safe and secure more easily, with customer and employee rights being respected according to GDPR.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects, in relation to the processing of personal data.

The GDPR brings in stronger legal protection for more sensitive information such as:

- Ethnic.
- Background.
- Political opinions.
- Religious beliefs.
- Health.
- Sexual health.
- Criminal records.

4. Responsibilities

The school must:

- Manage and process personal data properly
- Protect the individual's right to privacy

- Provide an individual with access to all personal data held on them.
- The school has a legal responsibility to comply with The Act. The school, as a corporate body, is named as the Data Controller under The Act.

Data Controllers are people or organisations who hold and use personal information. They decide how and why the information is used and have a responsibility to establish workplace practices and policies that are in line with The Act.

The school is required to 'notify' the Information Commissioner of the processing of personal data. This information will be included in a public register which is available on the Information Commissioner's website at the following link:
http://www.ico.gov.uk/what_we_cover/promoting_data_privacy/keeping_the_register.aspx

Every member of staff that holds personal information must comply with The Act when managing that information. The school is committed to maintaining the eight principles always. This means that the school will:

- Inform Data Subjects why they need their personal information, how they will use it and with whom it may be shared; this is known as a Privacy Notice
- check the quality and accuracy of the information held
- apply the records management policies and procedures to ensure that information is not held longer than is necessary
- ensure that when information is authorised for disposal it is done appropriately
- ensure appropriate security measures are in place to safeguard personal information whether that is held in paper files or on a computer system
- only share personal information with others when it is necessary and legally appropriate to do so
- set out clear procedures for responding to requests for access to personal information known as subject access in the Data Protection Act
- train all staff so that they are aware of their responsibilities and of the school's relevant policies and procedures

This policy will be updated as necessary to reflect best practice or amendments made to the Data Protection Act 1998.

Please follow this link to the ICO's website (www.ico.gov.uk) which provides further detailed guidance on a range of topics including individuals' rights, exemptions from the Act, dealing with subject access requests, how to handle requests from third parties for personal data to be disclosed etc. In particular, you may find it helpful to read the Guide to Data Protection which is available from the website.

5. Cloud services

We as a school are responsible for:

- Ensuring that the processing carried out by our cloud service provider complies with the DPA requirements by means of a contract and data processing agreement.

- Ensuring the accuracy of the self-certification statements made by the cloud services suppliers by using the self-certification checklists facilitated by the DFE.

6. School Practice

Within school we will, through appropriate management, strict application of criteria and controls:

- observe fully the conditions regarding the fair collection and use of information
- meet our legal obligations to specify the purposes, for which information is used
- collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements
- ensure the quality of information used
- apply strict checks to determine the length of time information is held
- ensure that the rights of people about whom information is held, can be fully exercised under the Act. (These include: the right to be informed that processing is being undertaken, the right of access to one's personal information, the right to prevent processing in certain circumstances and the right to correct, rectify, block or erase information which is regarded as wrong information)
- take appropriate technical and organisational security measures to safeguard personal information
- ensure that personal information is not transferred abroad without suitable safeguards
- treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information
- set out clear procedures for responding to requests for information

7. We will also ensure that:

- there is someone with specific responsibility for Data Protection within the school
- everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice
- everyone managing and handling personal information is appropriately trained to do so
- everyone managing and handling personal information is appropriately supervised
- anybody wanting to make enquiries about handling personal information knows what to do
- queries about handling personal information are promptly and courteously dealt with
- methods of handling personal information are clearly described
- a regular review and audit is made of the way personal information is held, managed and used
- methods of handling personal information are regularly assessed and evaluated
- performance with handling personal information is regularly assessed and evaluated
- a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against the members of staff concerned
- ensure that when information is authorised for disposal it is done appropriate.

8. Enquiries

Information about the school's Data Protection Policy is available from the Headteacher's PA. General information about the Data Protection Act can be obtained from the Data Protection Commissioner (Information Line 01625 545 745, website www.dataprotection.gov.uk).

9. Fair obtaining and processing

St Mary's CE Primary School undertakes to obtain and process data fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which the data are held, the likely recipients of the data and the data subjects' right of access. Information about the use of

personal data is printed on the appropriate collection form. If details are given verbally, the person collecting will explain the issues before obtaining the information.

"processing" means obtaining, recording or holding the information or data or carrying out any or set of operations on the information or data.
"data subject" means an individual who is the subject of personal data or the person to whom the information relates.
"personal data" means data, which relates to a living individual who can be identified. Addresses and telephone numbers are particularly vulnerable to abuse, but so can names and photographs be, if published in the press, Internet or media.
"parent" has the meaning given in the Education act 1996, and includes any person having parental responsibility or care of a child.

10. Registered purposes

The Data Protection Registration entries for the school are available for inspection, by appointment, at the school office. Explanation of any codes and categories entered is available from the Headteacher's PA who is the person nominated to deal with data protection issues in the school. Registered purposes covering the data held at the school are listed on the school's registration and data collection documents. Information held for these stated purposes will not be used for any other purpose without the data subject's consent.

11. Data integrity

The school undertakes to ensure data integrity by the following methods:

12. Data accuracy

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs the 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, the 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.

13. 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, the school will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data.

14. 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 School Business Manager and Headteacher's PA to ensure that obsolete data are properly erased.

15. Subject access

The Data Protection Act extends 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, the 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.

16. Processing subject access requests

Requests for access must be made in writing. Please see Appendix to School Policy on Data Protection.

17. Authorised disclosures

The school will, in general, only disclose data about individuals with their consent. However, there are circumstances under which the 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 the 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 demeanor within or in the vicinity of the 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 the 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 after permission from the Headteacher. Data used within the 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 the school who **need to know** the information in order to do their work. The 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.

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 the school, provided that the purpose of that information has been registered.

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 the School's registered purposes.

18. Data and computer security

St Mary's CE Primary School undertakes to ensure security of personal data by the following general methods.

19. Physical security

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

20. Logical security

Security software is installed on all computers containing personal data (Sophos Encryption). Only authorised users are allowed access to the computer files and password changes are regularly undertaken. Computer files are backed up (i.e. security copies are taken) regularly.

21. 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.

Overall security for data is determined by the Headteacher/Governing Body and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent.

Any queries or concerns about security of data in the school should in the first instance be referred to the Headteacher (the person responsible).

Individual members of staff can be personally liable in law under the terms of the Data Protection Acts and any breaches must be reported to the Information Commissions Office (ICO). 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.

When a new member of staff is assigned permissions in SIMS, it is the responsibility of the person assigning permissions to check that the permissions are appropriate and relevant to the post holder's responsibilities.

Further details on any aspect of this policy and its implementation can be obtained from: the Headteacher.

The following procedures have been agreed for responding to requests for Personal Information in accordance with the Data Protection Act 1998 and the GDPR 2018.

Anybody who makes a request to see their file or their child's file or other personal data held on them is making a request under the Data Protection Act 1998. All information relating to the child

including that held in day books, diaries and on electronic systems and email should be considered for disclosure.

There is a statutory exception to the above, where parents do have an automatic right to access defined materials under The Education (School Records) Regulations 1989. The school will observe these statutory rights.

If there is a current court order which relates to information regarding any child, that order must, regardless of other circumstances, be observed.

22. Dealing with a Data Protection Request

- A request under the Data Protection Act must be made in writing.
- In many cases a letter to the Headteacher will be sufficient to identify the information required. If you cannot identify the information required from the initial request, you can go back to the applicant to ask for more information.
- The Headteacher must be confident of the identity of the individual making the request This could be done by checking signatures against verified signatures on file or by asking the applicant to produce valid identification, such as a passport or photo-driving license. These checks should be done in addition to proof of relationship with the child.
- An individual only has the automatic right to access information about themselves, requests from family members, carers or parents of a minor will have to be considered. The Headteacher will have responsibility for ensuring the child's welfare is appropriately considered in deciding whether to comply with a request. Normally the requester will have to prove both their relationship with the child and that disclosure is in the child's best interests to the satisfaction of the Headteacher. In the event of a child having sufficient capacity to understand (normally age 12 or above) the Headteacher should discuss the request with the child and take their views into account when making a decision. There may be circumstance in which a child can refuse their consent to a request.
- The school may charge a statutory fee, currently calculated on a sliding scale, but only if a permanent copy of the information is provided. If a letter is sent out requesting a fee the 40-calendar day statutory timescale does not begin until the fee is received. It is important though that no request is delayed unnecessarily by time taken to inform the applicant of a fee.
- The school will make use of exemptions under the Act as appropriate. All files must be reviewed before any disclosure takes place. Under no circumstance will access be granted immediately or before this review process has taken place.
- Where information has been provided to the School by a third party, for example by the local authority, the police, a health care professional or another school, but is held on the school's file it is normal to seek the consent of the third party before disclosing information. This must be done early in the process in order to stay within the 40-day timescale. Even if the third party does not consent or consent is explicitly not given the data may be disclosed. In these cases, it may be appropriate to seek additional advice.
- The applicant should be told the data that the school holds, be given a copy of the data, and be told the purposes for which it is processed and whether it has been shared with any other party. It is good practice to explain whether data has been withheld and if so why. There may be circumstances where this is not appropriate; the Headteacher should at all times consider the welfare of the child. The school should also give details of who to contact in the event of a complaint and the details of the Information Commission who can provide independent information.

- Where all the data in a document cannot be disclosed a permanent copy should be made and the data obscured, or parts of the data can be retyped if this is more sensible. In any event a copy of the full document (before obscuring) and the altered document should be retained together with the reason why the document was altered. This is so, that in the event of a complaint, there is an audit trail of what was done and why.
- Information can be provided by post (registered mail) or on deposit at the school with an officer available to help the applicant. If the latter is used the applicant must have access to a photocopier in case they want a permanent copy of their data. In considering the method of delivery the views of the applicant should be taken into account. Any codes, technical terms or abbreviations should be explained. Any data which is difficult to read or illegible should be retyped.
- Schools should monitor the number of requests received and document whether they are dealt with within the 40-calendar day statutory timescale.
- The Act applies only to living individuals.

23. Complaints

Complaints about the operation of these procedures should be made to the Chair of the Governing Body who will decide if it is appropriate for the compliant to be dealt with under the complaints procedure. Complaints which are not dealt with under the school's complaint procedure should be forwarded in writing to the Information Commissioner. It is likely that complaints about procedural issues, due process and timeliness will be dealt with by the Governing Body, complaints that involve consideration of personal data or sensitive personal data should be referred to the Information Commissioner.

24. Contacts

Anyone with concerns or questions in relation to this policy should contact the Headteacher's PA om the first instance who will also act as the contact point for any requests under the Data Protection Act.

25. Linked policies

Network Access Policy
CCTV Policy
Freedom of Information Policy
Complaints Policy
DBS Statement
e-Safety Policy
Use of ICT, including social media, Policy

26. Equal Opportunities Statement

This policy applies to all users regardless of their special educational need, sexual orientation, culture, race, religion, belief, gender reassignment, ability or disability, preferred gender, ethnicity or nationality.

27. Monitoring and Review

This policy will be monitored by the school leadership team and reviewed biennially, or as new legislation determines, by the Governing Body in line with other data protection related policies.

Date: April 2018