St Mary's Church of England Primary School
Data Protection Policy Statement April 2018

1. Introduction and Scope

1.1 This policy is intended to ensure that personal data is dealt with properly and securely and in accordance with the law. 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

1.2 The Data Protection Act is the law that protects personal privacy and applies to any organisation which processes or has access to people's personal data. The Act helps ensure that the management of data held electronically and / or and in paper-based systems is processed correctly.

1.3 This policy sets out the framework for St Mary's School's compliance with Data Protection law St Mary's School has a privacy notice setting out how it uses pupil and parent data at the following website address

1.4 St Mary's School has a legal responsibility to comply with the Data Protection Act 2018, and with the requirements of the General Data Protection Regulation from 25 May 2018. The school, as a public authority, is named as the Data Controller under the Act. Data Controllers are organisations which hold and process personal data and have a duty to establish workplace practices and policies that are in line with the Act.

1.5 St Mary's is registered as a Data Controller with the Information Commissioner's Office (ICO), which regulates the Data Protection Act 2018, to confirm that information about individuals is being collected, processed and held. The registration number is ZA108280. Overall responsibility for Data Protection rests with the Governing Body; responsibility for securing compliance with the Data Protection Act and reporting this to the Governing Body is delegated to as, Senior Information Risk Owner.

1.6 St Mary's is obligated to have a Data Protection Officer in place under the law. The Data Protection Officer is the Camden Data Protection Team and they can be contacted at LB Camden.

1.7 This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the school. Any failures to follow the policy may result in disciplinary proceedings.

1.8 The school processes a large amount of personal data such as staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection etc. In addition, the school may be required by law to collect and use certain types of information to comply with statutory obligations of the local authority, government agencies or other bodies.

2. **Personal data**

2.1 Personal data is any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This means information about a living individual who can be identified from that data either by itself or alongside any other information we hold (e.g. name, address, date of birth, National Insurance number, bank account details). It includes any expression of opinion about that individual and any indication of any intentions the school has in respect of that individual and it also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings.

2.2 Personal data can also be considered to be Special Category Data as defined by the law. This is information about racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health or condition, sexual life, biometric data. Separate rules also apply in relation to information relating to criminal convictions. St Mary's School will only collect and process this information for specific purposes where allowed by the law (for example equal opportunities monitoring) or where it has asked and received consent to do so.

2.3 St Mary's School to follow the six principles set out in the law. The principles state that all personal information, or data, about individuals should be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

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

3. Information sharing and disclosure

3.1 St Mary's School shares personal data with other public authorities, including the London Borough of Camden and the Department of Education, where obliged to do so under law. An example of this is the school census return, which states which children are attending the school, their characteristics and the results of statutory or national testing. The school also has other legal responsibilities to share data about individuals, for instance, St Mary's School is required to report child protection concerns to the Multi-Agency Safeguarding Hub (MASH) for the borough in which the child is resident.

3.2 St Mary's School may also enter into a contractual arrangement with 3rd party organisations to carry out processing on its behalf (as Data Processors) or for professional advice to support the school's functions. Examples of this are management information and human resources systems, payments and IT providers and curricular software. Prior to entering into such an arrangement, St Mary's School will ensure that adequate security is in place to protect personal data and that adequate contractual terms are in place to ensure that the personal data transferred and/or collected by that 3rd party is only used for the purposes defined by St Mary's School. Prior to reaching such an arrangement, St Mary's School will conduct an assessment using the process set out under 6.2.

3.3 With the exception of the above, personal information will not usually be released to anyone else without the consent or knowledge of the individual. There are, however, certain circumstances when a third party (such as a government agency or law enforcement agency) can request information about individuals and we may be obliged to disclose it to them (for example where the disclosure is required by law or by a court order).

4. Individual rights

4.1 The law grants a number of individual rights. They are:

A. The right to be informed
B. The right of access
C. The right to rectification
D. The right to erasure
E. The right to restrict processing
F. The right to data portability
G. The right to object
H. Rights in relation to automated decision making and profiling.

4.2 **The right to be informed**

4.2.1 In order to meet the right to be informed, St Mary's School will ensure it gives adequate notice of why data is being collected and how it will be used. St Mary's School will publish a Privacy Notice on its website detailing its use of pupil/student data and issue a Privacy Notice to staff regarding the use of their data. It will issue further information when collecting data to ensure that there is clarity as to whether consent is required, that any consent gained is unambiguous, informed and freely given, and which individual rights may apply.

4.3 **The right of access**

4.3.1 Individuals ("Data Subjects") have the right to access their personal data. The person who the personal data is about is known as the data subject and the person who is making the request is known as the applicant. These can of course be the same person depending on the personal data sought. A common example of this relationship would be when a parent (applicant) is seeking personal information about their child (data subject).

4.3.2 To request access to all the personal data that the school holds about a Data Subject, a Subject Access can be completed and submitted to us. It is available at. A valid request can be made without submitting the form but further clarification may be required.

4.3.3 SECONDARY SCHOOLS ONLY Parents can generally request personal data about their child without their consent, however it should be noted that the Data Protection Act requires a data controller to assess the maturity and competency of a data subject which is not restricted to age. Therefore for pupils over 13, consent of the child may still be required.

4.3.4 To protect personal data when processing a request, the school may also require copies of two forms of identification. These should be:

- one piece of photographic identification, such as a valid passport, valid driving licence or a valid EU national identity card.
- one piece of identification confirming your address and dated within the last three months such as a utility bill, council tax statement or bank statement.

4.3.5 Applicants may book an appointment with via the School Office which will accept the application and validate the identification. Whilst St Mary's School may be able to confirm your identification in person, should you require any personal data be posted to you, the school will always require proof of address to ensure that any data that the school releases is sent securely and to the correct address. There may also be occasions where someone is legally allowed to act on behalf of someone else (for example power of attorney). The school will require proof of this prior to providing access to information.

4.3.6 Please note the school can charge a ‘reasonable fee’ when a request is manifestly unfounded or excessive, particularly if it is repetitive. The school may also charge a reasonable fee to comply with requests for further copies of the same information. The fee will be based on the administrative cost of providing the information.

4.3.7 Following receipt of a written request and identification being completed, will prepare the information requested within 30 calendar days. However, if St Mary’s School does not have the information required to perform a search, it will contact the applicant and ask for more details (The 30 day period of response will begin from the day we receive sufficient information to enable a search).

4.3.8 Requests for access to personal data will normally be carried out by the staff within the school. Where the input of the Data Protection Officer has been necessary, to clarify whether documents should be disclosed, this will be specified in the response.

4.3.9 A separate right exists under the Education (Pupil Information) (England) Regulations 2005 (SI 2005/1437) for parents to view their child’s Educational Record. Under the regulations, the school is entitled to levy a charge for a copy of the documents received. In light of the changes under the Data Protection Act 2018, the Governing Body has agreed that, on receipt of a request for the Educational Record, the school will provide a copy of a pupil’s educational record to the parent, free of charge, within fifteen school days of receipt of the parent’s written request for a copy of that record. Requests should be made to the Head of School via the School Office.

4.3.10 The unlawful obtaining or disclosure of personal data without consent of the Data Controller is an offence under the law.

4.4 **The rights to rectification and erasure**

4.4.1 St Mary’s School recognises that the personal data it keeps should be accurate and kept up to date, kept for no longer than necessary and used for the purpose to

4.4.2 If an applicant wishes to change the data held by the school, on them or their child, they should do this via the School Office. If judged necessary, the applicant may be asked to follow the procedure set out in 4.3.6 and 4.3.7.

4.4.3 Where the applicant requests to change data held by the school or to have that data erased, St Mary’s School will assess whether other conditions apply e.g. is the retention of the data necessary as a result of a legal requirement of a public authority or in defence of a future claim. Where the school cannot comply with the request, in part or in full, it will respond in writing giving the reason for refusal.

4.5 **The right to restrict processing**

4.5.1 The right to restrict processing may apply in the following circumstances:

4.5.1.1 Where an individual contests the accuracy of specified personal data, processing will be restricted until St Mary's School has verified the accuracy of the personal data.

4.5.1.2 Where an individual has objected to specific purposes and means of processing personal data (and where St Mary's School had previously judged that this was necessary for the performance of a public interest task), and St Mary's School is considering whether its legitimate grounds override those of the individual (further information is under 4.7)

4.5.1.3 If processing has been agreed by St Mary's School to be unlawful and the Data Subject (or their parent or guardian) opposes erasure and requests restriction instead.

4.5.1.4 If St Mary's School no longer requires the personal data but the Data Subject (or their parent or guardian) requires the data to establish, exercise or defend a legal claim.

4.5.2 Where one of the circumstances set out above applies, St Mary's School will put in place measures which ensure that processing of the personal data is restricted e.g. restricted access, suspension of processing.

4.6 **The right to data portability**

4.6.1 The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. The right to data portability only applies to data received from an individual, which is carried out on the basis of consent or legitimate interests and where the processing takes place via automatic means.

4.6.2 The right does not apply to data processed in performance of a public task

4.7 **The right to object**

4.7.1 Individuals have the right to object to processing based on the performance of a task in the public interest or the exercise of official authority.

4.7.2 St Mary's School will notify individuals of their right to object in its Privacy Notice and at the point of first communication where personal data is collected.

4.7.3 The right to object is individual and should be based on grounds relating to the individual's particular situation. Objections can be made via the School Office.

4.7.4 Where an objection is received, St Mary's School will cease the processing objected to (in relation to the individual only). However, it will retain the data until such time as it has been determined that the following exemptions do not apply:

4.7.4.1 compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or

4.7.4.2 the processing is for the establishment, exercise or defence of legal claims.

4.7.5 The Head of School will determine whether either exemption applies. Prior to reaching a decision determining that an exemption applies that overrules the right to object, the Head of School will will seek and have regard to the advice of the Data Protection Officer. The individual will be informed of the decision by the Head of School and their rights in writing within 5 working days of such a determination. Should the individual be dissatisfied with the outcome of this process, a further complaint may be made to the Governing Body or to the Information Commissioner's Officer.

4.8 **Rights in relation to automated decision making and profiling.**

4.9 St Mary's School does not carry out automated decision making and profiling as defined in the law.

5. Data Protection Officer

5.1 The role of the Data Protection Officer at St Mary's School is:

5.1.1 To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.

5.1.2 To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.

5.1.3 To be the first point of contact for supervisory authorities and for individuals whose data is being processed (employees, customers etc).

5.2 The Data Protection Officer reports to the Governing Body and will provide periodic reports regarding compliance.

5.3 Where changes to St Mary's School's means or purposes of processing personal data are proposed, the Head of School will ensure that an assessment of any impact on individual privacy is carried out (as set out in 6 below). Where appropriate, the Data Protection Officer will be consulted as part of this process and the Senior Information Risk Owner and the Governing Body will take account of any advice given.

5.4 Requests to exercise individual rights should be addressed in the first instance via the School Office which will be able to carry out routine requests. However, individuals may contact the Data Protection Officer at any time with concerns or to exercise their rights.

6. Privacy by Design and Default

6.1 St Mary's School has a general obligation under the law to implement technical and organisational measures to show that it has considered and integrated data protection into its processing activities.

6.2 Where changes to St Mary's School's means or purposes of processing personal data are proposed, the Head of School will ensure that an assessment of any impact on individual privacy is carried out (as set out in 6 below), using the process set out in Appendix A (Data Protection Impact Assessment). Where appropriate, the Data Protection Officer will be consulted as part of this process and the Head of School and the Governing Body (or the member of school staff with delegated responsibility for the decision) will take account of any advice given prior to implementing the proposed changes.

6.3 St Mary's School will also, with the input of the Data Protection Officer, implement a programme to ensure compliance with the Data Protection Act. This will include:

- e.g. Periodic training for staff and compulsory training for new starters
- e.g. Responsibilities in respect of Data Protection included in Staff Code of Conduct
- e.g. Maintaining processing records, in the form of an information asset register, detailing what personal data is held, where it is held and for how long
- e.g. Yearly review of this policy and associated documentation by the Governing Body
- e.g. Periodic reporting to the Governing Body by the Data Protection Officer on the school's overall compliance with the Data Protection Act, identifying any areas of concern and reviewing any breaches or potential breaches

7. Responsibilities for Information Security

7.1 As per the Data Protection Act and as a corporate body, the school is the Data Controller of the personal data it processes and Governors are therefore ultimately responsible for ensuring the school's compliance, however designated officers will deal with day to day matters.

7.2 St Mary's School will ensure that all personal data is accessible only to those who have a valid reason for using it and not disclosed to any unauthorised third parties. Any member of staff, parent or other individual who considers that this policy has not been followed in respect of personal data should raise the matter with Head of School and/or the Data Protection Officer, whose contact details are above.

7.3 The designated officer responsible for data control is the **Head of School**

8. Staff Responsibilities

8.1 All members of staff are responsible for ensuring that:-

8.1.1 Any personal data which they hold is kept securely.

8.1.2 Any information provided to the school in connection with their employment is accurate and up to date including informing of any changes to information which has been provided (for example changes of address) or any errors spotted.

8.1.3 Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party. (Unauthorised disclosure may result in disciplinary proceedings)

8.1.4 Any personal data held about other people or collected as part of their responsibilities (for example opinions on reports, references, marks, details of personal circumstances) is kept securely.

8.1.5 Personal data that is written, printed or in electronic format held on an unencrypted disk, USB / portable data transfer device or other removable storage media should be kept in a locked filing cabinet, locked drawer, safe or in a lockable room with key-controlled access. Records containing personal data must never be left where unauthorised personnel can read or gain access to them.

8.1.6 Computer screens, terminals, CCTV camera screens or any Visual Display Unit (VDU) that shows personal data should be placed so that they are not visible except to authorised staff. PC screens will not be left unattended without a password protected screen saver being used.

8.2 This policy also applies to staff and pupils who process personal data 'off-site' (for example when working at home). Staff are still responsible in such circumstances and additional care must be taken regarding the security of the

data. Any personal data, in any format, will not be taken off the school premises without approval of the Head of School

8.3 Under the law, any employee may be personally liable in a court of law for unauthorised disclosure of personal data.

8.4 It is also a criminal offence to gain unauthorised access to information on a computer system under the Computer Misuse Act 1990.

9. Closed Circuit Television

9.1 St Mary's School does not use Closed Circuit Television (CCTV).

10 Security Measures

Access to Data

10.1 Staff's access to personal data will be limited to that required for legitimate processing.

10.2 Staff, including volunteers and temporary staff, will be asked to confirm that they understand their responsibilities under section 9 of this document in writing prior to receiving access to personal data held by the school.

10.3 Staff will receive periodic training on handling personal data and on their responsibilities under the Data Protection Act.

Destruction and deletion of expired data

10.4 Expired records containing personal data will be disposed of securely, maintaining confidentiality. These records must be kept secure until it has been destroyed. Confidential waste sacks are available by contacting the school 020 7624 4837

10.5 Personal and sensitive personal data stored on computers or computer media, such as USB keys, CDs, cannot be securely removed by simple deletion or reformatting. Camden IT should be contacted to ensure the safe disposal of these devices.

10.6 In addition the school will put in place appropriate measures for the deletion of personal data. Manual records will be shredded or disposed of as '*confidential waste'*, CDs / DVDs / Disks should be cut into pieces, Audio / Video Tapes and (where applicable) Fax rolls should be dismantled / shredded. Hard drives of redundant PCs will be wiped clean before disposal, or, if that is not possible, destroyed physically.

10.7 Appropriate contract terms will be put in place with any third parties undertaking this work on the school's behalf.

10.8 The school will maintain a log of the records destroyed and who authorised their destruction to meet the requirements of the Freedom of Information Act 2000.

Security of physical records containing personal data

10.9 `Unauthorised staff and other individuals will be prevented from gaining access to personal information. Personal data is stored in locked cabinets, with keys held only by those members of staff who require access to that data for their duties. The school maintains a register of personal data held in physical formats and its location within the school.

Security of electronic records containing personal data

10.10 Personal data that is computerised should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. The school has/follows procedures to protect against data loss and intrusion, in conjunction with its IT providers.

10.11 The school has in place measures to protect personal data held electronically. Access to the school's systems and information contained within is access controlled, with each member of staff having a unique account and User ID with a password known only to them. Staff are reminded never to share details of their account, User ID or password

12 Data Breach Management Procedure

12.1 Appropriate measures are taken against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data by the school. This procedure will be followed in the event of a data security breach, examples of which are:

• Loss or theft of data or equipment on which data is stored on school premises or outside
• Inappropriate access controls allowing unauthorised use
• Equipment failure
• Human error - correspondence with personal data sent to the wrong email address
• Unforeseen circumstances such as a fire or flood
• Hacking attack
• 'Blagging' offences where information is obtained by deceit from the school

12.2 The school will follow the following steps if a data security or potential data security breach occurs:

1. **Detection**
When a member of staff becomes aware that a breach or potential breach has occurred, they must notify the SIRO and DPO as soon as possible.

2. Containment and recovery

- Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise
- Establish whether there is anything you can do to recover any losses and limit the damage the breach can cause.
- Where appropriate, inform the police
- Assess whether the breach should be reported to the ICO
- Notify the ICO within 72 hours of breach being detected if breach is identified as serious

3. Assessment of ongoing risk

The following points are also likely to be helpful in making this assessment:

- What type of data is involved – staff or pupil sensitive personal data
- Where personal data has been lost or stolen, are there any protections in place such as encryption?
- How many staff and/or pupils personal data are affected by the breach?
- What harm can be done to these individuals – risks to physical safety, reputation etc.

4. Notification of breach

The DPO and SIRO will arrange for those affected by the breach to be notified as soon as practically possible.

5. Evaluation and response

In the event of a breach, the DPO will complete an investigation as to the causes of the breach and also evaluate the effectiveness of the school's response to it. This will be reported to a Committee of the Governing Body and where necessary, the school will update its policies and procedures accordingly.

The school will maintain a log of breaches, specifying the nature of the incident and the response taken.

Last reviewed by Governing Body	Date / Term / Year
Next revision	Annual / Bi-annual / Tri-annual / Termly
To be reviewed	Date / Term / Year