Our Commitment to you

St Mary & St Michael Catholic Primary School is committed to ensuring the security and protection of the personal information that it process, and to provide a compliant and consistent approach to data protection.

As a School we have always ensured that we have had a strong Data Protection policy in place which complied with existing law. However, the School recognises the need to update this to ensure compliance with the General Data Protection Regulations 'GDPR' and the Data Protection Act 2018.

St Mary & St Michael Catholic Primary School strives to ensure the security of all the personal information in our possession and in setting up processes that are effective, fit for purpose and demonstrates an understanding of, and appreciation for the new Regulations .Our preparation and objectives for GDPR compliance have been summarised in this statement and include the development and implementation of new data protection roles, policies, procedures, controls and measures to ensure maximum and ongoing compliance.

How We Are Preparing for the GDPR

St Mary & St Michael Catholic Primary School already has a consistent level of data protection and security processes in place, however it is our aim to be fully compliant with the GDPR.

Our preparation includes: -

- Information Audit - carrying out an information audit to identify and assess what personal information we hold, where it comes from, how and why it is processed and if and to whom it is disclosed.

- Policies & Procedures – updating our policies and procedures to meet the requirements and standards of the GDPR and any relevant data protection laws, including: -

- Data Protection – our main policy and procedure document for data protection has been updated to meet the standards and requirements of the GDPR. Accountability and governance measures are in place to ensure that we understand and evidence our obligations and responsibilities; with a dedicated focus on privacy by design and the rights of individuals.

- Records Management - we have updated our retention policy and schedule to ensure that we comply with the relevant region period for data held.

- Data Breaches – our breach procedure ensures that we have the appropriate measures in place to identify, assess, investigate and report any personal data breach at the earliest possible time.

- Third-Party Disclosures - We will carry out strict checks with all recipients of personal data to assess and verify that they have appropriate safeguards in place to protect the information, ensure enforceable data subject rights and have effective legal remedies for data subjects where applicable.

- Subject Access Request (SAR) – we have revised our SAR procedures to accommodate the revised 30-day timeframe for providing the requested information and for making this provision free of charge. Our new procedures detail how to verify the data subject, what steps to take for processing an access request, what exemptions apply and a suite of response templates to ensure that communications with data subjects are compliant, consistent and adequate.

- Legal Basis for Processing - we have reviewed all processing activities to identify the legal basis for processing and ensuring that each basis is appropriate for the activity it relates to. Where applicable, we also maintain records of our processing activities, ensuring that our obligations under Article 30 of the GDPR and Schedule 1 of the Data Protection Bill are met.

- Privacy Notice/Policy – our Privacy Notice(s) comply with the GDPR, and ensure that all individuals whose personal information we process have been informed of why we need it, how it is used, what their rights are, who the information is disclosed to and what safeguarding measures are in place to protect their information.

- Obtaining Consent - We have a stringent process for recording consent, (where necessary) making sure that we can evidence an affirmative opt-in, along with time and date records; and an easy to see and access way to withdraw consent at any time.

- Data Protection Impact Assessments (DPIA) – where we process personal information that is considered high risk, involves large scale processing or includes special category/criminal conviction data; we have developed stringent procedures and assessment templates for carrying out impact assessments that comply fully with the GDPR's Article 35 requirements. We have implemented documentation processes that record each assessment, allow us to rate the risk posed by the processing activity and implement mitigating measures to reduce the risk posed to the data subject(s).

- Processor Agreements – where we use any third-party to process personal information on our behalf we have Data Sharing Agreements in place and procedures for ensuring that they meet and understand their/our GDPR obligations. These measures include initial and ongoing reviews of the service provided, the necessity of the processing activity, the technical and organisational measures in place and compliance with the GDPR.

- Special Categories Data - where we obtain and process any special category information, we do so in complete compliance with the Article 9 requirements and have high-level encryptions and protections on all such data. Special category data is only processed where necessary and is only processed where we have first identified the appropriate Article 9(2) basis or the Data Protection Bill Schedule 1 condition. Where we rely on consent for processing, this is explicit and is verified by a signature, with the right to modify or remove consent being clearly signposted.

Data Subject Rights

In addition to the policies and procedures mentioned above that ensure individuals can enforce their data protection rights, we provide easy to access information via of an individual's right to access any personal information that we process about them and to request information about: -

- What personal data we hold about them
- The purposes of the processing
- The categories of personal data concerned
- The recipients to whom the personal data has/will be disclosed
- How long we intend to store your personal data for
- If we did not collect the data directly from them, information about the source
- The right to have incomplete or inaccurate data about them corrected or completed and the process for requesting this
- The right to request erasure of personal data (where applicable) or to restrict processing in accordance with data protection laws, as well as to object to any direct marketing from us and to be informed about any automated decision-making that we use
- The right to lodge a complaint or seek judicial remedy and who to contact in such instances

Information Security & Technical and Organisational Measures

St Mary & St Michael Catholic Primary School takes the privacy and security of individuals and their personal information very seriously and take every reasonable measure and precaution to protect and secure the personal data that we process. We have robust information security policies and procedures in place to protect personal information from unauthorised access, alteration, disclosure or destruction and have several layers of security measures, including: -

GDPR Roles and Employees

St Mary & St Michael Catholic Primary School have designated the Schools Data Protection Officer (London Borough of Tower Hamlets) as our Data Protection Officer (DPO). The DPO is responsible for promoting awareness of the GDPR across the organisation, assessing our GDPR readiness, identifying any gap areas and implementing the new policies, procedures and measures, in conjunction with the St Mary & St Michael Catholic Primary School Leadership Team

St Mary & St Michael Catholic Primary School understands that continuous employee awareness and understanding is vital to the continued compliance of the GDPR and have involved our employees in our preparation plans. We have implemented an employee training program specific to the which will be provided to all employees and forms part of our induction and annual training program.

If you have any questions about our preparation for the GDPR, please contact the Schools Data Protection Officer at school.dpo@towerhamlets.gov.uk