St Mary's C E Primary School

St Mary's C E Data Protection Policy

"Live, Love and Learn Together in the Light of the Life of Christ"

1. About this document

This policy sets out how St Mary's C E Primary School complies with its obligations under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the Data (Use and Access) Act 2025, together with other relevant data protection legislation and statutory requirements.

The purpose of this policy is to ensure that personal data relating to pupils, parents and carers, staff, governors and other individuals is processed lawfully, fairly, transparently and securely, and in a manner that protects the rights and freedoms of individuals. The school will ensure that personal data is processed only where there is an appropriate lawful basis and in accordance with the data protection principles.

2. Scope

This policy applies to all personal data processed by St Mary's C E Primary School in carrying out its functions and activities, regardless of the format in which the information is held.

It applies to personal data relating to pupils, parents and carers, prospective pupils and their families, current and former employees, job applicants, governors, volunteers, contractors, visitors, suppliers and other individuals whose personal data is processed by the school.

This policy applies to personal data processed wholly or partly by automated means, including information held electronically, and to personal data processed by non-automated means, including paper records, where the information forms part of, or is intended to form part of, a structured filing system.

This policy applies to all staff, governors, volunteers, contractors and other individuals who process personal data on behalf of the school. All those covered by this policy are expected to understand and comply with their responsibilities when handling personal data.

The purpose of this policy is to:

- explain how the school complies with applicable data protection legislation;
- establish the responsibilities of those who process personal data on behalf of the school;
- explain how the school protects personal data and demonstrates accountability; and
- support and protect the rights of individuals in relation to their personal data.

This policy should be read alongside the school's related policies, procedures, privacy notices and other data protection documentation. Anyone who is unsure about the appropriate handling of personal data should seek advice from the school's Data Protection Lead or Data Protection Officer before taking action.

3. Policy statement

1. St Mary's C E Primary School, Garnet Road, London, NW10 9JA, is committed to protecting the personal data and the rights and freedoms of individuals whose information it collects and processes. The school will comply with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Data (Use and Access) Act 2025 and other applicable data protection legislation.

2. The school will maintain appropriate policies, procedures, technical and organisational measures, risk-management arrangements, training, monitoring and contractual arrangements to ensure that personal data is processed lawfully, fairly, transparently and securely and that the school can demonstrate its compliance with data protection legislation.

3. The school will regularly review its data protection arrangements and practices, and will update them where necessary to reflect changes in legislation, statutory guidance, regulatory guidance, technology, systems and the school's processing activities.

4. Compliance with data protection legislation is supported by this policy and the school's related policies, procedures, privacy notices, records, contracts and other data protection documentation.

5. The school will maintain an accurate and up-to-date Record of Processing Activities (RoPA), documenting its personal data processing activities as required by data protection legislation. The RoPA will be reviewed regularly and whenever significant changes are made to the school's processing activities, systems or arrangements. It will also be informed by relevant Data

Protection Impact Assessments (DPIAs) and will be made available to the Information Commissioner's Office (ICO) where required.

6. All staff, governors, volunteers, contractors and other individuals authorised to process personal data on behalf of the school must respect the confidentiality of personal data and access, use and disclose it only where they are authorised to do so and where it is necessary for the performance of their role.

7. All individuals working for or on behalf of the school are expected to comply with this policy and the school's associated data protection and information-security procedures. Failure to comply may result in action being taken under the school's relevant disciplinary or contractual procedures. Where a suspected breach may constitute a criminal offence or requires notification to a regulatory or other competent authority, the school will seek advice from its Data Protection Officer and take appropriate action in accordance with the law.

8. Where the school appoints a third party to process personal data on its behalf, it will use processors that provide sufficient guarantees that appropriate technical and organisational measures are in place to protect personal data and the rights of individuals. Appropriate written contracts or other legally binding arrangements will be put in place in accordance with data protection legislation. The school will undertake appropriate due diligence and will monitor processor compliance proportionately according to the nature and risk of the processing.

9. The school will have regard to relevant statutory guidance and to applicable guidance, codes of practice and regulatory advice issued by the Department for Education (DfE), the Information Commissioner's Office (ICO) and other relevant authorities.

10. The school does not currently use pupils' biometric data as part of an automated biometric recognition system. If the school proposes to introduce such a system in the future, it will comply with the UK GDPR, the Data Protection Act 2018, the Protection of Freedoms Act 2012 and relevant Department for Education guidance, including the requirements relating to notification, consent, pupil objections and the provision of reasonable alternative arrangements.

4. Responsibilities

Data protection is the responsibility of everyone who processes personal data on behalf of St Mary's C E Primary School. The school, as data controller, is responsible for ensuring that personal data is processed in accordance with applicable data protection legislation and for demonstrating its compliance with those requirements.

Governing Board

The Governing Board has overall responsibility for ensuring that the school complies with its legal obligations in relation to data protection and information governance. It provides strategic oversight and seeks assurance that appropriate policies, procedures, resources and controls are in place to protect personal data and the rights of individuals.

The Governing Board will:

- ensure that appropriate data protection policies and governance arrangements are in place and reviewed regularly;
- ensure that the school has appointed a suitably qualified Data Protection Officer (DPO), who is able to carry out the statutory functions of the role independently;
- seek appropriate assurance that data protection risks are identified and managed;
- ensure that appropriate arrangements are in place for staff training and awareness; and
- receive appropriate information about significant data protection risks, incidents and compliance matters.

Headteacher and Senior Leadership Team

The Headteacher and Senior Leadership Team are responsible for implementing the school's data protection arrangements and promoting a culture in which personal data is handled appropriately and securely.

They will:

- support the implementation of this policy and associated data protection procedures;
- ensure that staff understand their responsibilities and complete appropriate data protection training;
- ensure that appropriate technical and organisational measures are implemented to protect personal data;
- ensure that data protection risks are identified and appropriately managed;
- involve the Data Protection Lead and, where appropriate, the Data Protection Officer when new systems, technologies or processing activities are proposed;

- ensure that personal data breaches and suspected breaches are reported immediately in accordance with the school's data breach procedure; and
- support the timely handling of requests relating to individuals' data protection rights.

Subject Access Requests, requests relating to other individual rights, proposed data-sharing arrangements, Data Protection Impact Assessments (DPIAs), significant changes to the processing of personal data, and actual or suspected personal data breaches must be referred promptly to the Data Protection Lead and, where appropriate, the Data Protection Officer.

Data Protection Lead

The Data Protection Lead coordinates the school's day-to-day data protection arrangements and supports the Headteacher, Senior Leadership Team and staff in implementing this policy. The Data Protection Lead acts as the principal internal point of contact for routine data protection matters and liaises with the school's Data Protection Officer (DPO) where appropriate.

The Data Protection Lead will:

promote awareness of data protection requirements and good information-handling practice across the school;

provide day-to-day guidance to staff on the appropriate handling of personal data and seek advice from the DPO where necessary;

coordinate the school's procedures for responding to Subject Access Requests and requests relating to other individual rights;

support the maintenance and review of the school's Record of Processing Activities (RoPA), privacy notices and other data protection documentation;

coordinate Data Protection Impact Assessments (DPIAs) where required and seek the advice of the DPO;

support the assessment of proposed data-sharing arrangements, new systems, technologies and processing activities;

coordinate the recording, initial assessment and investigation of actual or suspected personal data breaches and ensure that significant incidents are referred promptly to the DPO;

support the provision and monitoring of appropriate data protection training and awareness for staff;

identify and escalate data protection risks or compliance concerns to the Headteacher, Senior Leadership Team and/or DPO as appropriate; and

report periodically to the Headteacher and Senior Leadership Team on data protection matters, including significant risks, incidents, requests and areas requiring action.

Data Protection Officer

The school will appoint a suitably qualified Data Protection Officer (DPO) in accordance with data protection legislation.

The Data Protection Officer will:

- inform and advise the school and its staff about their obligations under data protection legislation;
- monitor the school's compliance with data protection legislation and relevant policies, including through appropriate monitoring, awareness-raising and training;
- provide advice on Data Protection Impact Assessments (DPIAs) and monitor their performance where required;
- cooperate with the Information Commissioner's Office (ICO) and act as a contact point for the ICO on matters relating to the processing of personal data;
- provide advice on data protection risks, breaches, individual-rights requests, complaints and other significant data protection matters where appropriate; and
- be accessible to individuals in relation to matters concerning the processing of their personal data and the exercise of their rights.

The DPO will perform their statutory functions independently, will be appropriately involved in matters relating to the protection of personal data and will report to the highest management level of the school. The school will provide the DPO with the resources and access necessary to carry out the role and will ensure that the DPO is not instructed as to how to perform their statutory duties or placed in a position involving a conflict of interest.

Staff

All members of staff who process personal data as part of their work have a responsibility to handle that information lawfully, appropriately and securely and to comply with this policy and the school's associated data protection, information security and acceptable-use procedures.

Staff must:

- access, use and disclose personal data only where they are authorised to do so and where it is necessary for the performance of their role;
- maintain the confidentiality of personal data and not discuss or disclose confidential information to unauthorised individuals, including family members, friends or colleagues who do not have a legitimate need to know;
- take appropriate steps to prevent personal data from being seen, overheard, accessed, altered, lost or disclosed by unauthorised individuals;
- take appropriate care when communicating personal data by telephone, email, messaging systems or other means, including checking the identity of recipients where appropriate;
- use school-approved systems, devices and methods for storing, accessing, transmitting and sharing personal data and comply with the school's information-security and acceptable-use requirements;
- keep passwords and other authentication credentials secure and never share them with others;
- lock or log off devices when leaving them unattended and take appropriate precautions when working remotely or away from the school premises;
- ensure that personal data they create or record is accurate, relevant and kept up to date where this forms part of their role;
- follow the school's retention and secure-disposal arrangements and not retain personal data for longer than necessary or dispose of it without appropriate authority;
- cooperate promptly with requests from the Data Protection Lead, Data Protection Officer or other authorised staff relating to data protection matters, including Subject Access Requests and other individual-rights requests;
- complete required data protection and information-security training and apply that training in their work;

- report any actual or suspected personal data breach, loss of information, unauthorised disclosure, security incident or other data protection concern **immediately to the Data Protection Lead**, in accordance with the school's data breach procedure;
- inform the appropriate member of staff where they become aware that personal data held by the school may be inaccurate or out of date; and
- seek advice from the Data Protection Lead before processing, sharing or disclosing personal data where they are unsure whether it is appropriate to do so.

Failure to comply with this policy or associated procedures may be dealt with under the school's disciplinary procedures and, where appropriate, may also result in contractual, regulatory or legal action.

5. The Data Protection Principles

The UK GDPR sets out six data protection principles governing the processing of personal data. In addition, the accountability principle requires the school to be responsible for, and able to demonstrate, compliance with those principles. Personal data must therefore be:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation);
- adequate, relevant and limited to what is necessary for the purposes for which it is processed (data minimisation);
- accurate and, where necessary, kept up to date (accuracy);
- kept in a form that permits identification of individuals for no longer than is necessary (storage limitation);
- processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage (integrity and confidentiality); and
- processed in a way that enables the school to demonstrate compliance with these principles (accountability).

Lawfulness, fairness and transparency

Lawfulness – The school must identify and document an appropriate lawful basis before processing personal data. The appropriate lawful basis will depend on the purpose and circumstances of the processing.

Under the UK GDPR, the lawful bases for processing personal data are:

- consent;
- contract;
- legal obligation;
- vital interests;
- public task;
- recognised legitimate interests; and
- legitimate interests.

As a public authority, the school will commonly rely on **legal obligation** or **public task** when processing personal data as part of its statutory and official functions. The school will not rely on consent where individuals are not able to exercise a genuine and free choice.

Where the school processes **special category personal data** or **criminal offence data**, it will ensure that the additional conditions required by the UK GDPR and Data Protection Act 2018 are met and documented, where applicable.

Fairness – Personal data will be processed in ways that individuals would reasonably expect and will not be used in ways that have unjustified adverse effects on them. The school will consider the circumstances and potential impact of its processing, with particular care taken when processing children's personal data.

Transparency – The school will be open and clear about how and why it processes personal data. Privacy information will be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Where information is provided to children, the school will ensure that it is presented in an age-appropriate and accessible way.

The school will maintain and regularly review appropriate privacy notices for pupils and parents/carers, staff and other relevant individuals. Privacy notices will be reviewed whenever there is a significant change to the way in which personal data is processed.

In accordance with Articles 13 and 14 of the UK GDPR, privacy information will include, as applicable:

- the identity and contact details of the school as data controller;

- the contact details of the Data Protection Officer;
- the purposes for which personal data is processed and the applicable lawful basis;
- any legitimate interests relied upon, where applicable;
- the categories of personal data concerned, where applicable;
- the recipients or categories of recipients with whom personal data may be shared;
- information about international transfers and the safeguards used, where applicable;
- the period for which personal data will be retained, or the criteria used to determine that period;
- the rights available to individuals in relation to their personal data;
- the right to withdraw consent where processing is based on consent;
- the right to make a complaint about the school's processing of personal data and the right to complain to the Information Commissioner's Office;
- the source of personal data where it has not been obtained directly from the individual, where applicable;
- whether the provision of personal data is a statutory or contractual requirement and the possible consequences of failing to provide it, where applicable; and
- information about relevant automated decision-making, including profiling, where applicable.

Purpose limitation

Personal data will be collected for specified, explicit and legitimate purposes and will not be further processed in a manner that is incompatible with those purposes.

The school will clearly identify and document the purposes for which personal data is processed and will provide appropriate information about those purposes in its privacy notices and other relevant documentation.

Where the school proposes to use personal data for a new purpose, it will consider whether the new processing is compatible with the purpose for which the information was originally collected and will ensure that an appropriate lawful basis applies. Where required, the school will carry out and document a

compatibility assessment, update its privacy information and other relevant records, and seek advice from the Data Protection Officer.

The school will take account of circumstances in which data protection legislation provides that further processing may be treated as compatible with the original purpose, including relevant provisions introduced by the Data (Use and Access) Act 2025.

Data minimisation

Personal data processed by the school will be adequate, relevant and limited to what is necessary for the purposes for which it is processed.

The school will only collect and retain personal data that is reasonably necessary for an identified purpose. Staff must not collect, access, use or retain personal data merely because it may be useful at a later date.

Data collection methods, including forms, online systems, applications and new technologies, will be designed and reviewed to ensure that only necessary and relevant personal data is collected. Appropriate privacy information will be provided or made available to individuals at the point of collection or within the timescales required by law.

New or significantly changed systems, technologies or processing activities involving personal data must be considered from a data protection perspective at an early stage. The Data Protection Lead will be involved as appropriate and a Data Protection Impact Assessment (DPIA) will be undertaken where the processing is likely to result in a high risk to the rights and freedoms of individuals.

The school will review its data collection and processing activities regularly, and when significant changes occur, to ensure that the personal data it processes remains adequate, relevant and limited to what is necessary.

Personal data must not be kept for longer than necessary

Personal data will be retained only for as long as is necessary for the purposes for which it is processed, including where retention is required to meet legal, regulatory, safeguarding, financial, contractual or operational requirements.

The school will maintain and follow an appropriate Records Retention Schedule or Records Retention Policy which sets out the periods for which different categories of records should normally be retained.

When personal data is no longer required, it will be securely deleted, destroyed or anonymised, as appropriate, in a manner that prevents unauthorised access to or recovery of the information.

Where there is a legitimate reason to retain personal data beyond the school's usual retention period, the school will document the reason for the extended retention and keep the continued need for the information under review. Advice will be sought from the Data Protection Lead and/or Data Protection Officer where appropriate.

Personal data that must be retained will continue to be protected by appropriate technical and organisational measures throughout the retention period. Access will be limited to those who have an authorised and legitimate need to access it.

Personal data must be processed securely

Personal data will be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

The school will implement appropriate technical and organisational measures to protect personal data, taking into account the nature, scope, context and purposes of the processing, the risks to the rights and freedoms of individuals, and the likelihood and severity of potential harm.

Security measures will be proportionate to the risks presented by the processing and will include, where appropriate, measures relating to access controls, authentication, secure storage and transmission, encryption, backup and recovery, device and network security, staff training, physical security and the secure disposal of information.

The school will regularly review the effectiveness of its information-security arrangements and will assess data protection and security risks when introducing or significantly changing systems, technologies or processing activities.

Staff must comply with the school's information-security, acceptable-use and data-protection requirements and must report actual or suspected personal data breaches or security incidents immediately in accordance with the school's data breach procedure.

Further requirements relating to the security of personal data are set out in the **Security of Data** section of this policy and in the school's associated information-security policies and procedures.

When determining appropriate technical and organisational security measures, the school will take account of the nature, scope, context and purposes of the processing, the sensitivity and volume of the personal data, the risks to individuals, the state of the art and the cost of implementation.

Appropriate measures may include, according to the nature and risk of the processing:

- appropriate access controls and role-based permissions, based on the principle of least privilege;
- strong authentication and password-management arrangements, including multi-factor authentication where appropriate;
- automatic locking of unattended or inactive devices;
- encryption of personal data, devices and communications where appropriate;
- appropriate controls over removable media, portable devices and the downloading or transfer of personal data;
- appropriate network, endpoint, firewall, malware-protection, monitoring, backup and recovery arrangements;
- timely management of user accounts and access rights, including the prompt removal or amendment of access when staff, contractors or other users leave or change roles;
- appropriate physical security for devices, servers and paper records;
- secure configuration, updating and patching of systems and devices;
- pseudonymisation or anonymisation where appropriate;
- appropriate arrangements for securely deleting or disposing of personal data and equipment containing personal data;
- appropriate due diligence and contractual security requirements for processors, suppliers and cloud-based services; and
- relevant security standards and guidance issued by the National Cyber Security Centre (NCSC), Department for Education (DfE), Information Commissioner's Office (ICO) and other appropriate bodies.

The school will review its security arrangements regularly and following significant changes to systems, technologies, processing activities or identified risks. Appropriate specialist advice will be sought from the school's IT support provider, Data Protection Officer or other relevant professionals where necessary. The school will have regard to Department for Education Cyber Security Standards for Schools and Colleges and relevant National Cyber Security Centre guidance.

Organisational security measures

When determining appropriate organisational measures to protect personal data, the school will take account of the nature and sensitivity of the information, the risks associated with the processing and the roles and responsibilities of those who have access to personal data.

Appropriate organisational measures may include:

- ensuring that staff, governors and other relevant individuals receive appropriate data protection, information-security and cyber-security training and awareness;

- ensuring that individuals are appropriately vetted and authorised for their roles, in accordance with the school's recruitment, safeguarding and employment procedures;
- ensuring that confidentiality, data protection and information-security responsibilities are appropriately reflected in employment, contractual and other relevant arrangements;
- maintaining appropriate procedures for responding to breaches of this policy and, where applicable, addressing misconduct through relevant disciplinary or contractual procedures;
- monitoring and reviewing compliance with the school's data protection and information-security policies and procedures;
- applying appropriate physical access controls to areas, systems and records containing personal data;
- ensuring that paper records and portable devices containing personal data are stored securely when not in use;
- applying clear-desk and clear-screen practices where appropriate;
- establishing appropriate arrangements governing remote working and the use of portable, personal or privately owned devices;
- maintaining appropriate password, authentication and access-control procedures;
- maintaining appropriate backup, recovery and business-continuity arrangements;
- ensuring that access to personal data is limited to individuals who have an authorised and legitimate need to access it;
- ensuring that data protection risks are considered when procuring or introducing new systems, services, technologies and suppliers, including EdTech and artificial intelligence tools;
- ensuring that appropriate contracts and data-processing arrangements are in place with processors and other relevant third parties; and
- ensuring that appropriate safeguards and procedures are followed where personal data is transferred internationally.

These measures will be reviewed regularly and updated where necessary to reflect changes in risks, technology, systems, working practices, legislation and relevant guidance.

Accountability

St Mary's C E Primary School, as data controller, is responsible for complying with the data protection principles and must be able to demonstrate its compliance.

The school will maintain appropriate governance arrangements, policies, procedures, records and technical and organisational measures to demonstrate that personal data is processed in accordance with the UK GDPR, the Data Protection Act 2018 and other applicable data protection legislation.

The school will demonstrate accountability through measures including, where appropriate:

- maintaining and regularly reviewing data protection policies, procedures and privacy notices;
- maintaining an accurate and up-to-date Record of Processing Activities (RoPA);
- identifying and documenting appropriate lawful bases and, where applicable, conditions for processing special category or criminal offence data;
- implementing data protection by design and by default when developing or changing systems, services and processing activities;
- carrying out Data Protection Impact Assessments (DPIAs) where processing is likely to result in a high risk to the rights and freedoms of individuals;
- maintaining appropriate contracts and oversight arrangements with processors and other relevant third parties;
- maintaining records of personal data breaches and following appropriate breach assessment, reporting and notification procedures;
- providing appropriate data protection and information-security training and awareness for staff;
- maintaining appropriate procedures for handling Subject Access Requests, other individual-rights requests and data protection complaints;
- regularly reviewing data protection and information-security risks and the effectiveness of relevant controls; and
- seeking advice from the Data Protection Officer and involving the DPO appropriately and in a timely manner in matters relating to the protection of personal data.

6. Individual rights

Individuals, including children, have rights in relation to the personal data that the school processes about them. The availability and extent of some rights depend on the circumstances and the lawful basis on which the personal data is processed.

Subject to the conditions and exemptions set out in data protection legislation, individuals may have:

- **the right to be informed** about how and why the school collects and uses their personal data;
- **the right of access** to their personal data and to other information about how it is processed, usually by making a Subject Access Request (SAR);
- **the right to rectification** of inaccurate personal data and to have incomplete personal data completed where appropriate;
- **the right to erasure** of personal data in certain circumstances;

- **the right to restrict processing** of personal data in certain circumstances;
- **the right to data portability** in circumstances where the right applies;
- **the right to object** to processing in certain circumstances, including an absolute right to object to the use of personal data for direct marketing; and
- **rights and safeguards relating to solely automated decision-making, including profiling, where decisions produce legal or similarly significant effects.**

The school will facilitate the exercise of individual rights and will respond to valid requests within the timescales required by data protection legislation. Requests may generally be made verbally or in writing and do not need to use specific terminology or a particular form.

Staff who receive a request that may relate to an individual's data protection rights must pass it promptly to the Data Protection Lead so that it can be recorded and handled appropriately.

The school may need to verify the identity and, where relevant, the authority of the person making a request before disclosing or amending personal data. Any verification requested will be reasonable and proportionate to the circumstances.

Individual rights are not absolute and may be subject to conditions, limitations or exemptions under data protection legislation. Where the school decides not to act on a request, it will explain the decision as required by law and inform the individual of the relevant routes for complaint or challenge.

Automated decision-making

Where the school uses solely automated processing to make a decision that produces legal or similarly significant effects on an individual, it will ensure that an appropriate lawful basis applies and that the safeguards required by data protection legislation are provided.

These safeguards will include providing the individual with appropriate information about the decision and enabling them to make representations, obtain meaningful human intervention and contest the decision.

Additional restrictions apply where special category personal data is used for significant solely automated decision-making. The school will seek advice from the Data Protection Officer and undertake a Data Protection Impact Assessment where required before introducing such processing.

Subject Access Requests

Individuals have the right to request access to personal data that the school holds about them. A Subject Access Request may be made verbally or in writing and does not need to include the words "Subject Access Request" or "SAR".

The school will respond to Subject Access Requests without undue delay and normally within one calendar month, subject to any lawful extension, pause or adjustment to the response period.

In responding to a Subject Access Request, the school will carry out reasonable and proportionate searches for personal data within the scope of the request and will consider applicable exemptions and the rights of other individuals before information is disclosed.

Further information about the handling of Subject Access Requests is set out in the school's Subject Access Request Procedure.

Data protection complaints

Individuals have the right to raise concerns or complaints with the school about the processing of their personal data or the handling of an individual-rights request.

The school will provide an accessible means for individuals to make data protection complaints, including electronically. Complaints will be acknowledged within 30 days of receipt and appropriate steps will be taken to investigate and respond to them without undue delay.

Individuals will be informed of the outcome of their complaint and, where appropriate, of their right to complain to the Information Commissioner's Office (ICO) and to seek a judicial remedy.

Further information is set out in the school's Data Protection Complaints Procedure.

7. Consent

The school will rely on consent as a lawful basis for processing personal data only where it is appropriate to do so and where individuals are offered a genuine choice and control over the use of their personal data.

Consent must be freely given, specific, informed and unambiguous and must be indicated by a clear affirmative action. Consent will not be inferred from silence, inactivity, pre-ticked boxes or a failure to respond.

Where the school relies on consent, it will:

- clearly explain what personal data will be processed, the purpose of the processing and any relevant sharing of the information;
- ensure that consent is separate from other matters where appropriate and is presented in clear and accessible language;
- keep appropriate records demonstrating who consented, when and how consent was obtained, and what information was provided at the time;
- ensure that individuals are informed of their right to withdraw consent;
- make it as easy to withdraw consent as it was to give it; and
- stop the relevant processing when consent is withdrawn, unless there is another lawful basis that permits the continued processing or retention of the information.

Consent will not normally be relied upon where the school is required to process personal data to comply with a legal obligation or to perform its statutory or public functions, or where the circumstances mean that consent cannot be freely given.

Where special category personal data is processed, the school will identify both an appropriate lawful basis under Article 6 of the UK GDPR and an appropriate condition under Article 9. **Explicit consent** may be used as the Article 9 condition where appropriate, but it is not required where another applicable condition permits the processing.

Children's consent

Children have rights in relation to their own personal data. Where the school proposes to rely on a child's consent, it will consider whether the child has sufficient understanding and competence to understand what they are being asked to agree to and the consequences of their decision. Information and consent requests directed to children will be presented in clear, age-appropriate and accessible language.

Where an information society service is offered directly to a child and consent is relied upon as the lawful basis for processing, a child aged 13 or over may provide their own consent. Where the child is under 13, consent must be given or authorised by a person with parental responsibility, and reasonable efforts must be made to verify that authorisation, unless an applicable legal exception applies.

The school will take particular care when relying on consent in relation to children and will consider whether another lawful basis is more appropriate in the circumstances.

Use of Artificial Intelligence (AI)

The school recognises that artificial intelligence (AI) tools may be used to support educational and administrative activities. AI tools must be approved by the school before use where personal data may be processed.

Staff must not enter personal data, special category data, safeguarding information or confidential school information into unapproved AI systems or public generative AI platforms.

The school will assess AI systems for data protection, security, safeguarding and compliance risks and will undertake a Data Protection Impact Assessment where required.

Outputs generated by AI must be reviewed by an appropriately authorised member of staff before being relied upon for educational, safeguarding, employment or administrative decisions.

The school will have regard to relevant Department for Education, Information Commissioner and National Cyber Security Centre guidance relating to AI technologies.

8. Security of Data

St Mary's C E Primary School will implement appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing and against accidental loss, destruction, alteration, disclosure or damage.

Security measures will be proportionate to the nature and sensitivity of the personal data, the circumstances in which it is processed and the risks to the rights and freedoms of individuals.

Access to personal data

Access to personal data will be limited to individuals who are authorised to access it and who have a legitimate need to do so in order to carry out their role.

Access rights will be allocated according to role and will be reviewed and amended where appropriate, including when an individual changes role or leaves the school.

Staff must not access personal data merely because they are technically able to do so.

Personal data may only be disclosed or shared where there is an appropriate lawful basis or other legal authority for doing so and in accordance with the school's data-sharing arrangements and procedures.

Electronic information

Personal data held electronically must be protected by appropriate security measures. These will include, where appropriate:

- secure user accounts and authentication arrangements;
- strong passwords and multi-factor authentication where appropriate;
- appropriate role-based access controls;
- automatic locking of unattended or inactive devices;
- encryption of devices, information and communications where appropriate;
- appropriate network, firewall, malware-protection, monitoring, updating and patching arrangements;
- secure backup and recovery arrangements; and
- appropriate controls over removable media and the downloading, copying or transfer of personal data.

Staff must take reasonable steps to prevent personal data displayed on screens from being viewed by unauthorised individuals and must lock devices when leaving them unattended.

Staff must comply with the school's Acceptable Use Policy and other relevant information-security requirements when using school systems, devices and information.

Paper records

Paper records containing personal data must be stored securely and must not be left where they can be accessed or viewed by unauthorised individuals.

Particularly sensitive or confidential paper records must be kept in appropriately secure storage when not in use, with access restricted to authorised individuals.

Paper records must not be removed from the school premises unless there is a legitimate reason for doing so and appropriate security arrangements are in place.

Remote and off-site working

Personal data processed away from the school premises must be protected to an equivalent appropriate standard. Staff must follow the school's requirements relating to remote working, portable devices, personal devices, secure access and the transportation of paper or electronic records.

Personal data must not be stored, transferred or shared using personal email accounts, unauthorised cloud-storage services, applications, messaging

services, artificial intelligence tools or other systems that have not been approved for school use.

Secure disposal

Personal data will be securely deleted, destroyed or anonymised when it is no longer required, in accordance with the school's Records Retention Schedule or Records Retention Policy.

Paper records containing confidential or personal information will be securely destroyed, for example through confidential waste arrangements or cross-cut shredding where appropriate.

Devices and storage media containing personal data must be securely erased, sanitised or destroyed, as appropriate, before disposal, reuse or transfer, in accordance with the school's IT and asset-disposal arrangements.

Third-party systems and suppliers

Where a third party processes personal data on behalf of the school, the school will undertake appropriate due diligence and ensure that appropriate contractual and security arrangements are in place. The school will use processors that provide sufficient guarantees that appropriate technical and organisational measures are in place to protect personal data.

Staff must use only school-approved systems and services for processing personal data and must seek appropriate advice before introducing or using a new system, application, online service, EdTech product or artificial intelligence tool involving personal data.

Security incidents

Any actual or suspected loss, unauthorised disclosure, access, alteration or destruction of personal data, or other information-security incident involving personal data, must be reported **immediately to the Data Protection Lead** in accordance with the school's personal data breach procedure.

9. Sharing and Disclosure of Personal Data

The school will only share or disclose personal data where there is an appropriate lawful basis or other legal authority for doing so and where the sharing is necessary, proportionate and consistent with data protection legislation.

Before sharing personal data, the school will consider, as appropriate:

- the purpose for which the information is being shared;

- the lawful basis for the sharing and, where special category or criminal offence data is involved, any additional condition required;
- whether the information is necessary and proportionate for the intended purpose;
- who requires the information and whether their identity and authority to receive it have been appropriately verified;
- what information needs to be shared and whether the amount of personal data can be minimised;
- whether the information can be shared securely;
- whether the sharing is consistent with the school's privacy information and other relevant policies and procedures; and
- whether the sharing should be recorded or supported by a data-sharing agreement or other appropriate documentation.

Personal data must not be disclosed to family members, friends, other parents, members of the public or other unauthorised individuals merely because they request it or claim a relationship with the individual concerned.

Staff must take particular care to verify the identity and authority of individuals requesting personal data and must seek advice from the Data Protection Lead where they are unsure whether information can lawfully be disclosed.

Safeguarding

Data protection legislation does not prevent the appropriate sharing of personal data for safeguarding purposes. Where there is a safeguarding concern, the safety and welfare of the child will be the primary consideration and relevant information may be shared with appropriate agencies and professionals where there is a lawful basis for doing so.

Consent is not normally required where information needs to be shared in order to safeguard or protect a child. Safeguarding information will be shared in accordance with the school's Safeguarding and Child Protection Policy and applicable statutory guidance.

Decisions about the sharing of safeguarding information will normally be made or overseen by the Designated Safeguarding Lead (DSL) or an appropriately authorised deputy, and appropriate records will be maintained of significant information-sharing decisions.

Statutory and public-authority disclosures

The school may share personal data with organisations including the Department for Education, local authorities, other schools, children's social care, health services, safeguarding partners, law-enforcement agencies, courts and other public authorities where the school is legally required or permitted to do so.

Where a request for personal data is received from the Police or another law-enforcement agency, the school will consider the request on its individual circumstances and establish the appropriate legal basis before disclosing personal data. The identity and authority of the person making the request will be verified and the school will retain an appropriate record of the request and its decision.

Staff must refer unusual, complex or uncertain requests for disclosure to the Data Protection Lead, Designated Safeguarding Lead and/or Data Protection Officer, as appropriate.

If CCTV or similar surveillance technology is introduced, the school will undertake any required Data Protection Impact Assessment, provide appropriate signage and privacy information, establish retention periods and access controls, and comply with UK GDPR, the Data Protection Act 2018 and relevant ICO guidance. A separate CCTV policy will be adopted where appropriate.

The school does not currently operate CCTV or other surveillance systems that record identifiable individuals. The school is currently considering the future introduction of CCTV to support site security and safeguarding.

CCTV and Surveillance Systems

Staff must use only approved school systems and equipment when capturing, storing or sharing images or recordings containing personal data.

The school may create or use photographs, video recordings and other images for educational, safeguarding, administrative, celebratory and promotional purposes. The school will ensure that images are used lawfully, fairly and securely and that safeguarding considerations are taken into account.

Photography, Video Recording and Media Use

10. Retention and Disposal of Personal Data

St Mary's C E Primary School will retain personal data only for as long as it is necessary for the purposes for which it is processed, including where retention is necessary to meet legal, regulatory, safeguarding, financial, contractual or operational requirements.

The school will maintain a Records Retention Schedule or Records Retention Policy setting out the normal retention periods for different categories of records. Retention periods will take account of applicable statutory and regulatory requirements, relevant limitation periods, safeguarding requirements and recognised records-management guidance, including relevant recommendations in the IRMS Schools Toolkit where appropriate.

Retention periods will be reviewed when there are relevant changes to legislation, statutory guidance, the purposes for which information is processed or the school's systems and working practices.

Personal data may be retained for longer where there is a lawful and documented reason for doing so. This may include circumstances where information is required for safeguarding purposes, legal proceedings or anticipated legal claims, regulatory requirements, ongoing investigations, or archiving in the public interest, scientific or historical research, or statistical purposes in accordance with data protection legislation.

Where personal data is retained beyond its usual retention period, the reason for doing so will be documented and the continued need for retention will be kept under review. Appropriate technical and organisational measures will continue to protect the information throughout the retention period.

When personal data is no longer required, it will be securely deleted, destroyed or anonymised as appropriate. Paper and electronic records, devices and storage media containing personal data will be disposed of using methods appropriate to the sensitivity of the information and which prevent unauthorised access to or recovery of the data.

Staff must not destroy, delete or alter records that are subject to a current Subject Access Request, Freedom of Information request, safeguarding requirement, investigation, complaint, legal proceedings, anticipated legal claim or other requirement to preserve the information.

11. International Transfers of Personal Data

The school will ensure that any international transfer of personal data complies with the requirements of the UK GDPR, the Data Protection Act 2018 and other applicable data protection legislation.

Before making a restricted international transfer of personal data, the school will establish whether the UK GDPR international-transfer rules apply and will ensure that an appropriate transfer mechanism is in place.

Where required, the school will rely on an appropriate mechanism permitted by data protection legislation, which may include:

- UK adequacy regulations;
- appropriate safeguards, such as an approved International Data Transfer Agreement (IDTA), UK Addendum or other legally recognised safeguard; or
- an applicable exception permitted by data protection legislation in appropriate circumstances.

Where appropriate safeguards are relied upon, the school will undertake and document any required transfer risk assessment and apply the relevant data protection test, together with any additional measures necessary to protect the personal data.

The school will take particular care when procuring or using cloud-based services, EdTech, artificial intelligence tools and other systems where personal data may be accessed, stored, processed or supported from outside the UK.

The school will undertake appropriate due diligence and ensure that relevant contracts and data-processing arrangements identify and appropriately address international transfers, including transfers involving subprocessors.

Staff must not introduce or use systems or services that involve the international transfer of personal data without appropriate school authorisation and consideration of the applicable data protection requirements. Advice will be sought from the Data Protection Officer where appropriate.

12. Record of Processing Activities and Data Protection Impact Assessments

Record of Processing Activities (RoPA)

St Mary's C E Primary School will maintain an accurate and up-to-date Record of Processing Activities (RoPA) in accordance with Article 30 of the UK GDPR.

The RoPA will document the school's personal data processing activities and will include, as applicable:

- the name and contact details of the school as data controller and the contact details of the Data Protection Officer;
- the purposes of the processing;
- the categories of individuals whose personal data is processed;
- the categories of personal data processed;
- the categories of recipients to whom personal data is or may be disclosed;
- details of relevant international transfers and applicable safeguards;
- the envisaged retention periods, or relevant retention arrangements, for different categories of personal data; and
- a general description of the technical and organisational security measures used to protect personal data.

The school may also document or link the RoPA to other relevant information, including:

- the lawful basis for processing and, where applicable, conditions for processing special category or criminal offence data;
- privacy notices;
- data-processing agreements and other relevant contracts;
- information about systems, suppliers and processors;
- data flows and locations in which personal data is held;
- Data Protection Impact Assessments;
- records relating to consent, where consent is relied upon; and

- records of personal data breaches.

The RoPA will be reviewed regularly and updated whenever there are significant changes to the school's processing activities, systems, suppliers or arrangements. Relevant staff must provide information reasonably required to enable the school to maintain an accurate record.

The RoPA will be made available to the Information Commissioner's Office (ICO) where required.

Data Protection Impact Assessments (DPIAs)

The school will consider data protection risks at an early stage when proposing new or significantly changed processing activities, systems, technologies or services.

A Data Protection Impact Assessment (DPIA) will be carried out before processing begins where the proposed processing is likely to result in a high risk to the rights and freedoms of individuals.

In determining whether a DPIA is required, the school will take account of the nature, scope, context and purposes of the processing and relevant regulatory guidance. Particular consideration will be given to processing involving children or other vulnerable individuals, special category or criminal offence data, systematic monitoring, profiling or automated decision-making, innovative technologies, large-scale processing, matching or combining datasets, or other processing that may present a high risk.

Where appropriate, DPIAs will also be considered when procuring or making significant changes to EdTech, artificial intelligence tools, filtering and monitoring systems, CCTV or other technologies involving personal data.

A DPIA will:

- describe the proposed processing and its purposes;
- assess the necessity and proportionality of the processing;
- identify and assess risks to the rights and freedoms of individuals;
- identify measures to eliminate, reduce or manage those risks; and
- document the outcome, decisions, responsibilities and any actions required before the processing begins.

The Data Protection Officer will be consulted and their advice sought where required in relation to a DPIA. Relevant stakeholders, including the Data Protection Lead, IT support, Designated Safeguarding Lead and other appropriate staff or specialists, will be involved according to the nature of the proposed processing.

DPIAs will be kept under review and updated where there are significant changes to the nature, scope, context or purposes of the processing or where new risks are identified.

Where a DPIA identifies a **residual high risk that cannot be sufficiently reduced or mitigated**, the school will consult the Information Commissioner's Office before commencing the processing, in accordance with Article 36 of the UK GDPR. The school will not begin the relevant processing until the requirements relating to prior consultation have been addressed.

13. Personal Data Breaches

The school will maintain procedures for identifying, reporting, investigating, assessing, recording and responding to actual or suspected personal data breaches.

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

All staff, governors, volunteers and other individuals working on behalf of the school must report any actual or suspected personal data breach **immediately to the Data Protection Lead**, in accordance with the school's personal data breach procedure. Staff must not delay reporting while attempting to investigate or resolve the incident themselves.

Examples of incidents that must be reported include:

- personal data being sent or emailed to the wrong recipient;
- loss or theft of a device, document or other record containing personal data;
- unauthorised access to personal data or a school system;
- accidental deletion, alteration or loss of personal data;
- inappropriate disclosure of confidential or personal information;
- compromised passwords or user accounts where personal data may be at risk;
- cyber incidents affecting the confidentiality, integrity or availability of personal data; and
- any other incident that may have resulted in personal data being accessed, lost, disclosed, altered or destroyed without appropriate authority.

The Data Protection Lead will coordinate the initial recording and assessment of the incident and will seek advice from the Data Protection Officer where appropriate. Relevant staff, including IT support, the Designated Safeguarding Lead and senior leaders, will be involved according to the nature and severity of the incident.

The school will document personal data breaches, including the facts relating to the breach, its effects and the remedial action taken, regardless of whether the breach is reported to the Information Commissioner's Office (ICO).

Where a personal data breach is **likely to result in a risk to the rights and freedoms of individuals**, the school will notify the ICO without undue delay and, where feasible, no later than **72 hours after becoming aware of the breach**. Where notification is made after 72 hours, the reasons for the delay will be documented and provided to the ICO as required.

Where a personal data breach is **likely to result in a high risk to the rights and freedoms of individuals**, the school will also communicate the breach to the affected individual or individuals without undue delay, unless an applicable exception applies.

The school will take appropriate steps to contain and mitigate personal data breaches, reduce the risk of harm to individuals, recover or secure affected information where possible, preserve relevant evidence, and address any weaknesses identified as a result of the incident.

Where a processor or other supplier processing personal data on behalf of the school becomes aware of a personal data breach affecting school data, it must notify the school without undue delay in accordance with applicable contractual and data protection requirements.

Significant personal data breaches will be reviewed to identify lessons learned and any necessary improvements to policies, procedures, systems, security controls or staff training.

14. Data Protection Concerns and Complaints

Individuals who have a concern or complaint about the way in which the school has processed their personal data, or about the handling of a request relating to their data protection rights, are encouraged to raise the matter with the school so that it can be considered and, where appropriate, resolved.

The school will provide an accessible means for individuals to make a data protection complaint, including an electronic means of doing so. Complaints may be referred to the Data Protection Lead, who will coordinate their handling and seek advice from the Data Protection Officer where appropriate.

The school will:

- acknowledge receipt of a data protection complaint within 30 days;
- take appropriate steps to investigate the complaint without undue delay;

- make appropriate enquiries into the subject matter of the complaint;
- keep the complainant informed of the progress of the investigation where appropriate; and
- inform the complainant of the outcome without undue delay.

Appropriate records will be maintained of data protection complaints and their handling.

Where an individual remains dissatisfied with the school's response, they may complain to the Information Commissioner's Office (ICO). Individuals may also have the right to seek a judicial remedy through the courts.

Further information about making a data protection complaint and the school's arrangements for handling complaints is available in the school's Data Protection Complaints Procedure and/or relevant privacy information.

15. Further Information

Related policies and procedures

This policy should be read alongside the school's other relevant policies, procedures and documentation, including, where applicable:

- Information Security Policy;
- Access Control Policy;
- Acceptable Use Policy;
- Records Retention Schedule or Records Retention Policy;
- Personal Data Breach Procedure;
- Subject Access Request Procedure;
- Data Protection Complaints Procedure;
- Safeguarding and Child Protection Policy;
- relevant privacy notices;
- Data Protection Impact Assessment Procedure; and
- other relevant information-governance, cyber-security and IT policies and procedures.

Data Protection Officer (DPO): [Deepti Baal, deepti@educationadvisoryservice.org]

Further information and advice

Staff who require advice about data protection or the handling of personal data should contact the school's Data Protection Lead in the first instance.

Advice may also be sought, where appropriate, from

- the school's Data Protection Officer;
- the Headteacher;
- the school's IT support provider or other relevant specialist advisers; and

- the Local Authority or legal advisers, where appropriate.

Individuals may obtain independent information about their data protection rights from the Information Commissioner's Office (ICO).

Appendix 1 — Glossary

Personal data – any information relating to an identified or identifiable living individual. An identifiable individual is someone who can be identified, directly or indirectly, including by reference to information such as a name, identification number, location data, online identifier or one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity.

Special category data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; genetic data; biometric data where processed for the purpose of uniquely identifying an individual; data concerning health; or data concerning an individual's sex life or sexual orientation.

Data controller – the person or organisation that, alone or jointly with others, determines the purposes and means of processing personal data. St Mary's C E Primary School is a data controller in relation to the personal data for which it determines why and how it is processed.

Data processor – a person or organisation that processes personal data on behalf of a data controller and in accordance with the controller's instructions, subject to applicable legal requirements.

Data subject – the identified or identifiable living individual to whom personal data relates.

Processing – any operation or set of operations performed on personal data, whether or not by automated means, including collecting, recording, organising, structuring, storing, adapting, retrieving, consulting, using, sharing, disclosing, combining, restricting, erasing or destroying personal data.

Profiling – automated processing of personal data to evaluate certain personal aspects relating to an individual, particularly to analyse or predict aspects concerning their performance, economic situation, health, personal preferences or interests, reliability, behaviour, location or movements.

Personal data breach – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. All personal data breaches must be recorded by the school. A breach must be reported to the ICO where it is likely to result in a risk to the rights and freedoms of individuals,

and affected individuals must also be informed without undue delay where the breach is likely to result in a high risk, subject to applicable legal exceptions.

Consent – any freely given, specific, informed and unambiguous indication of an individual's wishes by which they, through a statement or clear affirmative action, signify agreement to the processing of personal data relating to them. Where explicit consent is required, a higher standard applies. Consent must be capable of being withdrawn.

Child – for the purposes of data protection legislation, children are individuals whose personal data is entitled to particular protection. There is no general requirement under the UK GDPR for parental consent before a school may process a child's personal data; the school must identify an appropriate lawful basis for the processing. Where an information society service is offered directly to a child and consent is relied upon as the lawful basis, a child aged 13 or over may provide their own consent. Where the child is under 13, consent must normally be given or authorised by a person with parental responsibility, subject to applicable exceptions.

Third party – a person, public authority, agency or other body other than the individual, controller, processor or persons who, under the direct authority of the controller or processor, are authorised to process the personal data.

Filing system – any structured set of personal data that is accessible according to specific criteria, whether held centrally, in different locations or organised on a functional or geographical basis.

Data Protection Officer (DPO) – the person appointed to carry out the statutory functions of the DPO under data protection legislation, including advising the school about its obligations, monitoring compliance, advising on DPIAs and acting as a contact point for the ICO. The DPO performs their functions independently.

Data Protection Lead – the person designated by the school to coordinate its day-to-day data protection arrangements and act as the principal internal point of contact for routine data protection matters.

Data Protection Impact Assessment (DPIA) – a documented process used to identify and assess data protection risks associated with processing that is likely to result in a high risk to individuals and to identify measures to reduce or manage those risks.

Record of Processing Activities (RoPA) – the school's record of its personal data processing activities maintained in accordance with Article 30 of the UK GDPR.