St Matthew's Westminster

Data Protection Policy

This policy was approved by the Governing Body in November 2022
This policy was reviewed by governors in December 2023
The next date for review will be November 2024
(unless any changes are necessary prior to this date)

BELONGING | BELIEVING | ACHIEVING

"You are the light of the world."
Matthew 5:14

Contents

1. Aims

St Matthew's CE Primary School (The School) aims to ensure that all personal data collected, stored, processed and destroyed about any natural person, whether they be a member of staff, pupil, parent, Governor, visitors, contractor, consultant, a member of supply staff or other individual in the school is done so in accordance with the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, collected, stored, processed, and destroyed in the school, regardless of whether it is in paper or electronic format, or the type of filing system it is stored in, and whether the collection or processing of data was, or is, in any way automated.

2. Legislation and guidance

This policy meets the current requirements of Data Protection legislation. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and DPA 2018. It is also based on the information provided by the Article 29 Working Party.
It also meets the requirements of the Protection of Freedoms Act 2012, ICO's code of practice in relation to CCTV usage, and the DBS Code of Practice in relation to handling sensitive information. This policy also complies with the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Term	**Definition**
Data controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, following the Controller's instruction.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Consent	Freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Personal data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a ● name, ● an identification number, ● location data, ● an online identifier or ● to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: ● Racial or ethnic origin ● Political opinions ● Religious or philosophical beliefs ● Trade union membership ● Genetics ● Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes ● Health – physical or mental ● Sex life or sexual orientation ● history of offences, convictions, or cautions * * Note: Whilst criminal offences are not listed as special category data, within this policy they are regarded as such in acknowledgment of the extra care which is needed with this data set.
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction. Processing can be automated or manual.
Data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

The School processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller and a data processor.

The School is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required, the registration number is **Z9618698.**

5. Roles and responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governing Body

The Governing Body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 Data Protection Officer

As a public body the School has appointed Grow Education Partners Ltd as its Data Protection Officer (DPO), the responsible contact is Claire Mehegan, claire.mehegan@london.anglican.org.

They are responsible for overseeing the implementation of this policy in the first instance, before reviewing our compliance with data protection law, and developing related policies and guidelines where applicable.

Upon request the DPO can provide an annual report of the school's compliance and risk issues directly to the governing board and will report to the board their advice and recommendations on school data protection issues.

The DPO is a named point of contact for all Data Subjects whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their SLA for Service.

5.3 Representative of the data controller

The Executive Headteacher (Sarah Maltese) acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff (regardless of role) are responsible for:

- Collecting, storing, and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, e.g. a change of address, telephone number, or bank details.
- Reporting a Data Breach, Data Right Request, or Freedom of Information Request.
- Contacting the DPO:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

Data Protection is based on seven principles that the School must comply with.
These are that data must be;

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

The Accountability principles ties these all together by requiring an organisation to take responsibility for complying with the other six principles. Including having appropriate measures and records in place to be able to demonstrate compliance.

This policy sets out how the school aims to comply with these key principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of six lawful bases (legal reasons) to do so under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**
- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)

For special categories of personal data, we will also meet one of the special category conditions for processing which are set under data protection law.

These are where:

- The individual (or their parent / carer in the case of a pupil, where appropriate) has **given explicit Consent;**
- It is necessary for the purposes of carrying out the **obligations and exercising specific rights** of the controller or of the data subject in the field of **employment** of a Data Controller or of a Data Subject;
- It is necessary to protect the **vital interests** of the Data Subject;
- Processing is carried out in the course of its **legitimate activities** with appropriate safeguards by a **foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim.**
- The Personal Data has **manifestly been made public** by the Data Subject;
- There is the **establishment, exercise or defence of a legal claim**;
- There are reasons of **public interest** in the area of **public health**;
- Processing is necessary for the purposes of preventative or occupational medicine (e.g. for the **assessment of the working capacity of the employee**, the medical diagnosis, the provision of health or social care or treatment);
- There are **archiving** purposes in the **public interest**;

Where we collect personal data directly from individuals, we will provide them with the relevant information required by data protection law, in the form of a privacy notice.

These privacy notices can be found on the school website or via the school office (office@stmwschool.org.uk)

- Pupils and Parents/Carers:
- School Workforce:
- Governors & Volunteers:
- Job Applicants:
- Suppliers/Contractors/Consultants:
- Visitors:
- Additional Copies of the Privacy Notices are available on request by contacting the school office (office@stmwschool.org.uk)

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data in our privacy notices.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.
Staff must only access and process personal data where it is necessary in order to do their jobs.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

When personal data is no longer required, staff must ensure it is deleted. This will be done in accordance with the school document retention policy, which states how long particular documents should be kept, and how they should be destroyed.

Copies of the Document Retention Policy can be obtained by contacting the school office.

8. Sharing personal data

In order to efficiently, effectively and legally function as a data controller we are required to share information with appropriate third parties, including but not limited to situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies or services – we may seek consent when appropriate before doing this where possible.
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law and have satisfactory security measures in place.
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share.
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and government bodies when required to do so, these include but are not limited to:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the United Kingdom or European Economic Area, we will do so in accordance with data protection law.

9. Individuals Data Protection Rights

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to access personal information that an organisation holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

While the school will comply with Data Protection legislation in regard to dealing with all Subject Access requests submitted in any format, individuals are asked to submit their request by letter or email addressed or marked for the attention of the School Business Manager (office@stmwschool.org.uk), St Matthew's CE Primary School, 18 Old Pye Street, London SW1P 2DG.

They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request, they must immediately forward it to the School Business Manager.

9.2 Children and Data Requests

An individual's data belongs to them; therefore, a child's data belongs to that child, and not the child's parents or carers.

However, children below the age of 12 are not generally regarded to be mature enough to understand their rights and the implications of invoking a data request. Therefore, for children under the age of 12 most data requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Where a child is judged to be of sufficient age and maturity to exercise their rights and a request is invoked on their behalf, we would require them to give consent to authorise the action to be undertaken.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification from the list below
    - passport
    - driving licence
    - utility bills with their current address
    - Birth / Marriage certificate
    - P45/P60

    - credit card or mortgage statement
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within the required regulatory timeframe.
- Will provide the information free of charge (unless it is found to be onerous, excessive or unfounded). Any fee charged will be reasonable and would only account for the administrative costs incurred while complying with the request.
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this as soon as possible, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual; or
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests; or
- Is contained in adoption or parental order records; or
- Is given to a court in proceedings concerning the child

If the request is manifestly unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which would only take into account administrative costs.
A request will be deemed to be manifestly unfounded or excessive if it is repetitive or asks for further copies of the same information.

In the event we refuse a request, we will tell the individual why, and tell them they have the right to refer a complaint to the ICO.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time, this only relates to tasks which the school relies on consent to process the data.
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it in certain circumstances and where sufficient supporting evidence is supplied
- Prevent the use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest, official authority or legitimate interests.
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area

- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Request a cease to any processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals have the right to exercise these rights at any point. Requests should be submitted to the School Business Manager.

If staff receive such a request, they must immediately forward it to the School Business Manager.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

Requests should be made in writing to the School Business Manager (office@stmwschool.org.uk), St Matthew's CE Primary School, 18 Old Pye Street, London SW1P 2DG, and should include;

- Name of individual
- Correspondence address
- Contact number and email address

11. Closed Circuit Television (CCTV)

The school uses CCTV to reduce crime and monitor the school buildings in order to provide a safe and secure environment for pupils, staff and visitors, and to prevent the loss or damage to school property. We adhere to the ICO's code of practice for the use of CCTV and provide training to staff in its use.

We do not need to ask individuals' permission to use CCTV, but in most instances we make it clear where individuals are being recorded, with security cameras that are clearly visible and accompanied by signage at entrances to the school explaining that CCTV is in use, and where it is not clear, directions will be given on how further information can be sought.

The system comprises 10 fixed cameras covering entrances, the playgrounds and the school office and main lobby. The system does not have sound recording capability.

The CCTV system is owned and operated by the school, and its deployment is determined by the Executive Headteacher.

The CCTV is monitored centrally from the school office and CCTV warning signs are displayed at the three entrance points of the school. All retained data will be stored securely.

Access to recorded images will be restricted to those staff authorised to view them, and will not be made more widely available.

Subject Access Requests (SAR):
Individuals have the right to request access to CCTV footage relating to themselves under the Data Protection Act. All requests should be made in writing to the Executive Headteacher. Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time and location. The school will respond to requests within 40 calendar days of receiving the written request and fee. A fee of £20 will be charged for each request. The school reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.

Access to and Disclosure of Images to Third Parties:
There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and service providers to the school where these would reasonably need access to the data (e.g. investigators).

The data may be used within the school's discipline and grievance procedures as required, and will be subject to the usual confidentiality requirements of those procedures.

Enquiries about the operation of CCTV within the school should be directed to the Executive Executive Headteacher in the first instance.

12. Photographs and videos
As part of our school activities, we may take photographs and record images of individuals within our school.

The use of school photographs includes but is not limited to:

- Within school on notice boards and in school magazines, brochures, newsletters and prospectuses.
- Outside of school by external agencies and partners such as the school photographer, local and national newspapers and local and national campaigns we are involved with

- Online on our website or social media pages

We will obtain consent from the responsible individuals in order to use photos and images. When doing so we will explain how the photograph and/or video will be collected and used by both the parent/carer and pupil when obtaining consent. Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

You can withdraw consent by contacting the school in writing at any point.

When using photographs and videos we will not accompany them with any other personal information about the child except their first name without explicit permission.

See our Child Protection and Safeguarding Policy on the school website for more information on our use of photographs and videos.

13. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data collection and processing activities. These include, but are not limited to the following organisational and technical measures:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection regulations.
- Completing data privacy impact assessments where the school's processing of personal data presents a high risk to the rights and freedoms of individuals, and when introducing new technologies or processing tools advice and guidance will be sought from the DPO.
- Integrating data protection into internal documents including this policy, and any related policies and privacy notices.
- Regular training for the school workforce on data protection law, this policy and any related policies and any other data protection matters. Records of attendance to ensure that all data handlers receive appropriate training.
- Periodic audits will be undertaken to monitor and review our privacy measures and make sure we are compliant.
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school's DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)

- For all personal data that we hold; maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

14. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular our organisational and technical measures include;

- Paper-based records and portable electronic devices, such as laptops, tablets and hard drives that contain personal data will be kept under lock and key when not in use
- Papers containing confidential personal data will not be left out on display when not in use unless there is a compelling lawful basis to do so e.g. displaying allergy information about children in the Staff Room.
- Staff are encouraged to set strong passwords (eg at least 8 characters long containing letters and numbers) and are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment, as set out in the school's *Online Safety and Acceptable Use Agreement.*
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

15. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will be corrected or updated, unless it is no longer of use in which case it will be disposed of securely.

For example, we will shred paper-based records, and overwrite or delete electronic files. We may also use a third party to dispose of records securely on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law and provide a certificate of destruction.

When records are disposed of as part of the Data Retention schedule the fact will be recorded on the school's Record of Destruction log.

16. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

All potential or confirmed Data Breach incidents should be reported to the Executive Headteacher or School Business Manager where they will be assigned a unique reference number and recorded in the school's Data Breach log.

Once logged, incidents will be investigated, the potential impact assessed, and appropriate remedial action undertaken. The DPO will be consulted as required.

Where appropriate, we will report the data breach to the ICO and affected Data Subjects within 72 hours.

The full procedure is set out in the School Breach Management Procedure.

Examples of a Data Protection Breach include but are not limited to:

- Personal data being left unattended in a meeting room/in the staffroom/in the PPA room
- Sending information relating to a pupil or family to the wrong member of staff in school, or to the wrong parent
- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

17. Monitoring arrangements

The Executive Headteacher is responsible for monitoring and reviewing this policy as part of the general auditing and compliance work which they carry out.

This policy will be reviewed yearly, and changes recommended by the DPO and others when appropriate. The Governors will be asked to approve the policy review and any necessary changes.

18. Links with other policies

This data protection policy is linked to our:

- Online Safety and Acceptable Use Policy
- Data Retention Policy
- Breach Management Procedures
- Asset Management Recording System

- Disaster Recovery/Business Continuity Planning and Risk Register.
- Child Protection and Safeguarding Policy