Data Protection Policy

St Martins C of E Primary School

Version 4

(This policy has been adopted from SIPS)

Date of last review:	August 2025
Date of this review:	August 2026
Date of next review:	August 2028

Policy Section	Page
Purpose	**4**
Introduction	**4**

Definitions and Common Terminology	**4-5**
Data Protection Principles and the Data Processing Measures used to comply with the GDPR:	**5-6**
Legality Transparency and Fairness Data mapping document Privacy notices Rights of a data subject	**5-6**
Purpose Limitation	**7**
Minimisation	**7**
Accuracy	**8**
Integrity and Confidentiality Clear desk and clear screen Passwords and protection of hardware Accessing and sharing information Cyber security Sharing of personally identifiable information Storage of data on portable/external devices Paper and manual filing systems Security of equipment and documents off school/academy premises Physical security Use of fax CCTV Staff use of work devices Use of AI software	**9-14**
Accountability Data protection officer and data protection lead Staff and governor training Third party organisations Data protection impact assessments Responsibilities	**14-15**
Photographs and Videos	**15-16**
Data Security and Storage of Data	**16**
Subject Access Requests How to request access to data and responding to a subject access request.	**16-19**
Data Breaches Responding to a data breach	**19**
Contact Details	**19-20**

Purpose

St Martins C of E Primary School Data Protection Policy is intended to ensure that personal information is dealt with securely and in accordance with the Data Protection Act 2018, UK General Data Protection Regulation (GDPR). It will apply to all data held by the school regardless of the way it is used, recorded and stored and whether it is held by the school in paper files or electronic form.

Introduction

The General Data Protection Regulation (GDPR) forms part of the Data Protection Act 2018. This regulation identifies certain principles that any organisation who stores or processes 'Personally Identifiable Information' must be able to demonstrate compliance with. The GDPR applies to all electronic and manual data files containing personally identifiable information (PII) or sensitive data.

St Martins C of E Primary School collect and use certain types of personal information about pupils, parents, staff, volunteers, governors, job applicants and other individuals who come into contact with the school in order to provide education, employment and other associated functions. Our school is required by law to collect and use certain types of information to comply with statutory obligations related to education, safeguarding and employment, and this policy is intended to ensure that personal information is dealt with securely and in accordance with the GDPR.

This policy has been put into place to ensure all Staff and Governors who process PII in the school understand the scope of the regulation, how it affects them, and the working practices that must be employed on a day-to-day basis in order to safeguard the personal information of individuals, which we have and use within the school. St Martins C of E Primary School will take reasonable steps to ensure that members of staff will only have access to personal data where it is necessary for them to carry out their duties. All staff will be made aware of this policy and their duties under the GDPR and should ensure they refer to this policy when carrying out their duties. St Martins C of E Primary School will take all reasonable steps and apply robust procedures to ensure that all PII is held securely and is not accessible to unauthorised persons.

This policy meets the requirements of the GDPR and the expected provisions of the Data Protection Act 2018. It is based on guidance published by:

- The Information Commissioner's Office (ICO)
- Department for Education's (DfE): Data Protection in School`s (2024)
- DfE's: Keeping Children Safe In Education (2024).

This policy will be updated when amendments to the data protection legislation are made or to reflect best practice where necessary. The policy will be reviewed every 2 years.

Definitions and Common Terminology

- ***Data Controller*** – a natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. The school is a data controller for the purposes of GDPR.
- ***Data Processor*** – a natural or legal person, public authority, agency or any other body that processes personal data on behalf of the data controller. This applies to third party organisations who process data on behalf of the school.
- ***Data Subject*** – an identified or identifiable living individual whose personal data is held or is processed. In relation to school this includes, staff, parents, carers, pupils, volunteers, governors, visitors etc.
- ***Personally Identifiable Information*** – any information relating to an identified or identifiable, living individual.
- ***Personal Data*** – examples of personal data include a name or title; contact details; information about behaviour and attendance; assessment and exam results; staff recruitment information and references.
- ***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. School specific data will also include information about safeguarding, pupil premium, special educational needs and disabilities, looked after children and children in need.
- ***Data Protection Officer*** – a person who is tasked with helping to protect personally identifiable information and helping an organisation to meet the GDPR compliance requirements, does not hold ultimate accountability for compliance.
- ***Subject Access Request*** – a right that a person has to obtain a copy of information held about them by the organisation.
- ***Data Breach*** – a breach of security leading to data being lost or stolen, destroyed or changed without consent or accessed by someone without permission. Data breaches can be deliberate or accidental.
- ***ICO*** – Information Commissioners Office (Supervising Authority in the UK)

Principles and How St Martins C of E Primary School Complies

In accordance with the obligations placed upon the school as a Data Controller, personal data will be processed in accordance with the Principles of GDPR. The following section outlines how St Martins C of E Primary School processes personal data in line with the GDPR guiding principles as follows:

(1) Legality, Transparency and Fairness: *Personal data will only be processed by the school, where it is able to demonstrate that it has a 'Lawful Basis' for the processing activity. Personal data will be processed fairly, and the school are open and honest about the uses of personal data.*

All personal data must be processed using at least one lawful basis, such as:

- Consent (permission has been given)
- Contract (necessary for a new/existing contract)
- Legal obligation (to comply with the law)
- Vital interests (to protect someone's life)
- Public task (for official functions/tasks in the public interest)
- Recognised legitimate interest (safeguarding, emergencies, preventing crime, etc)

A data mapping document is a 'live' document that records all data processed by the school. A 'Lawful Basis' is recorded against each data set to evidence and record a legal reason for collecting, processing, sharing, storing, and destroying data. Decisions regarding lawful basis are reviewed periodically.

The data mapping document will be held by the School Business Manager. All staff will be required to assist periodic reviews of the data mapping document to ensure all data sets currently in use within the school have been considered, captured, and a lawful basis for processing has been identified on each occasion.

A Privacy Notice details the school's use of personal data, including what PII is held by the school, how it will be stored, the organisations that data will be shared with, the lawful basis for processing and how long the data will be held for prior to destruction. Our data mapping document informs the content of our privacy notices. It also contains information regarding how a data subject (pupil, parent, member of staff etc) can access their data, which is stored and processed by the school.

In accordance with the principal of transparency, the school has developed and will maintain privacy notices for different categories of data subject. These outline the categories of data captured, the purpose of processing and if the information is shared with third party organisations.

Privacy notices for the following categories of data subjects and details of where this information is available, is as follows:

- Pupils, Parents and Carers: available via: school website
- Staff: available via internal shared area
- Visitors and Contractors: available via school website
- School Governors: available via school website
- Job Applicants: available via school website

A Data Subjects Rights

Under the GDPR, data subjects have the following rights with regards to their personal information, as follows:

1. Right to be informed about the collection and the use of their personal data
2. Right of access personal data and supplementary information
3. Right to have inaccurate personal data rectified or completed if it is incomplete.

4. Right to erasure (to be forgotten) in certain circumstances.
5. Right to restrict processing in certain circumstances
6. Right to data portability, which allows the data subject to obtain and reuse their personal data for their own purposes across difference services.
7. Right to object to processing in certain circumstances.
8. Rights in relation to automated decision making and profiling.
9. Right to withdraw consent at any time (where relevant)
10. Right to complain to the Information Commissioner

Individuals can submit a request to exercise the above rights to the Data Protection Lead in school. This may be done verbally or in written form. If staff receive such a request, they will immediately forward it to the Data Protection Lead, who will liaise with the Data Protection Officer as necessary. See section 8 for details of how a data subject can exercise their right to access their personal data.

(2) Purpose Limitation: *Personal data should be collected for specific, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.*

A data mapping document will identify the purposes for which processing will take place, the description of the categories of individuals and personal data, the categories of recipients of the data (e.g., Third party organisations who the school shares the data with). Retention schedules for the personal data will also be noted.

Appropriate technical and organisational measures must be in place to safeguard personal data and ensure PII is only used for the purpose for which it was collected.

(3) Minimisation: *The personal data must be 'Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.'*

Data collection forms and processes will be regularly reviewed to ensure information is appropriate and not excessive. Data required by teaching staff will be provided only for the purpose it is required to ensure data used is minimal.

If a member of staff wishes to introduce the use of new technology that captures personally identifiable information, they will first speak with the data protection lead in school. The Data Protection Lead will ensure appropriate measures, including completion of a data Protection Impact assessment prior to approval of a project and identify the appropriate lawful basis. The data mapping document will be updated accordingly.

Wherever there is any uncertainty about the level of information being requested from Data Subjects, a referral will be made to the Data Protection Lead/Officer for further guidance.

(4) Accuracy: *All reasonable steps will be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.*

Data will be proactively and regularly checked to ensure it is as accurate as possible through a variety of measures:

- Issuing data capture forms on an annual basis to parents/carers to verify the accuracy of personal information held on the SIMS system, including emergency contact details; correspondence address; medical details of the pupils etc.
- During termly parents' evenings
- Termly newsletters to remind parents to update their data if required.
- Use of apps such as ParentLite to allow parents real-time access to the data held on Arbor;
- Checking the accuracy of data during contact with parents including first day calling conversation via SENCO etc.
- Checking attainment data in systems on a regular basis, through the use of pupil progress meetings;
- Checking accuracy of staff details via *Arbor and staff files*

(5) Storage Limitation: *Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.*

Retention periods for various data held in the school are recorded within the data mapping document. The school refer to the Information Record Management Toolkit to establish appropriate retention periods and data is archived and destroyed as set out in these guidelines.

Personal data that is no longer required either due to it being out of date, inaccurate or in line with the school retention policy, will be disposed of securely. Records of disposal are maintained for accountability, i.e. certificate of destruction from shredding companies or record log completed by school.

Electronic files are deleted appropriately in line with retention periods. Data within emails (either as text or attached documents) are identified by content and filed into the relevant system, where it is then stored and destroyed in line with retention periods.

Paper-based records are shredded. School may also use a third-party organisation to safely dispose of records on the school's behalf. If so, a third-party assurance certificate will be obtained to provide school with sufficient guarantees that the company complies with data protection law.

Archiving: School will archive staff and student files in lockable cabinets onsite and will clearly label these with the year that they can be destroyed in line with retention periods. School uses a shredding company that destroy documents at the end of their lifespan.

(6) Integrity and Confidentiality: *Personal data will be processed in a manner which ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage, using appropriate technical or organisational measures.*

Staff have access to a number of policies, operational procedures and guidance to give them appropriate direction on processing data. This includes documents such as:

- Retention Policy
- CCTV Policy

(a) Clear desk and clear screen:

- PCs must not be accessible to others. All electrical devices including laptops, iPads, school mobile phones must not be left unlocked when workstations/classrooms are left unattended.
- Computer screens will be positioned to ensure only authorised personnel are able to view sensitive or confidential information. This is of particular importance within areas accessed by members of the public, such as the reception area or main school office. Privacy screens will be used where positioning of screens is not possible.
- Any paper-based documents containing personally identifiable information will be secured in a lockable cabinet or cupboard when classrooms / offices are left unattended and always at the end of the day. Data will not be displayed on notice boards. Where there are any concerns over the availability of secure (lockable) storage, or clarification required over the type of information that needs to be secured, staff will speak with the Data Protection Lead in the first instance, who will liaise with the Data Protection Officer if required.

(b) Passwords and protection of hardware:

- Passwords for accessing systems will be complex enough to make it extremely difficult for third parties to break them: passwords will be at least 8-10 characters long, have a mixture of upper case and lower-case letters, at least one number and one character. Where applicable a two-step authenticator app will be used to ensure an extra layer of security.
- Passwords will not be shared with any other member of staff / shared amongst other users or written down.
- Mobile devices (including phones, tablets and laptops) will be protected to the same high standard. School staff will:
- Activate the built-in security PIN and set this to the most secure level (if the device allows, this will always be a secure password as detailed above or fingerprint recognition rather than a 4-digit pin;
- A copy of the IMEI numbers for the phone and the SIMS are stored securely to allow deactivation in the event of loss.
- All school staff are personally responsible for any information accessed or disclosed on the devices they access. Therefore, passwords will be kept safe and secure, and will not be shared with anyone else, as outlined above.

(c) Accessing and sharing information:

- Electronic data will only be accessed via school devices. Staff are not permitted to access emails or personal data via their own devices, including mobile phones, laptops, iPads/tablets etc. Refer to the ICT Acceptable Use Policy.
- Staff will follow the secure process of accessing data via a secure function via OneDrive and how to safely download, modify, save and send data securely.

- Personal data will not be downloaded onto a personal mobile device without a justified clear business case for doing so and prior management approval. Downloaded data will automatically save to the device and therefore, if approval has been granted the data must be deleted immediately when it is no longer required.

(d) Cyber Security

- Measures such as encryption and access control are in place to prevent unauthorised access to the school network.
- Cyber security training and briefings are shared with staff to raise awareness and keep staff informed of the risks and procedures in place to protect data
- The cloud provider shares responsibility for the protection of data and assurances have been received.

(e) Sharing of Personally Identifiable Information.

- **Inside the School:** Information of a confidential, sensitive or personal nature will only be shared with staff who require access to the information. Where data has been shared via email the data will be deleted by all staff once it has been used for the purpose it has been collected and is no longer required.
- **Outside the School:** Where more than one piece of personal, sensitive or confidential data is to be sent, one of several methods will be used. If in doubt staff will check with the Data Protection Lead.
- Secure transmission: Where possible, use recognised secure electronic exchange programmes.
- Never send personal data within a normal email. If email is the only method of transmission available, ensure the information is included in a password protected document. The password must be agreed with the email recipient in advance either face to face or via telephone. The password will not be shared in a follow-on email. The password will not be included in the email to which the password protected document is attached (if the first email is intercepted, then the second could also be).
- Checks will be carried out prior to data being shared with third parties as to the purpose and only appropriate data will be provided. Staff will check with the Data Protection Lead before any data is shared.
- Data will be checked for accuracy and to ensure it is current prior to sending.
- School emails will never be sent to individuals within an organisation using a public email address (e.g., Hotmail, Gmail etc.) regardless of what they contain, unless this has been clearly identified by the recipient as their business email address and prior approval given by school SLT.
- Emails sent to a number of recipients will be checked for accuracy prior to sending. Parent's emails addresses will be inserted into the blind copy (BCC) section of the email to protect individuals contact details being shared.
- When sending information (including letters) via post the following process will be followed:
- A second person will always check the address is correct prior to sending. Particular attention to house numbers is required as these are easily transposed. However, the responsibility for the accuracy is still with the sender not the checker.

- Window envelopes will be used if the address is pre-populated on the enclosed letter to avoid transcription errors. Where plain envelopes are used typed labels will be used to avoid issues in relation to legibility of handwritten.
- Envelopes will be securely sealed. Using additional methods such as sticky tape, glue or staples if deemed necessary.
- The contents of the letter will be double checked to ensure that no additional information has been included that is not relevant e.g., something mistakenly attached or personal data of another individual. Only relevant data will be sent.
- The document will be checked for validity and accuracy.
- If a request is received from an outside agency such as the Police, this will be referred in the first instance to the Data Protection Lead.

(f) Storage of Data on Portable/External Devices

- The loss of any device that can send, store or retrieve data will be reported to your Data Protection Lead and the Data Protection Officer immediately.
- All devices provided by school to include mobile phone, laptop, memory stick, tablet, external hard drive, computer etc, will be encrypted, and care must be taken to safeguard the equipment against loss or damage. The password used to encrypt information will not be written down and will never be stored or transported with the device. Staff are reminded to change their passwords at regular intervals if a forced change of password is not set.
- All devices provided by the school will only be used for the purposes for which they were supplied.
- Unencrypted memory sticks to store data are not permitted by the school. Memory sticks that do not require a password to access the data contained on it will not be used and are not permitted by the school.
- Any storage devices no longer required, which may contain information that is surplus to requirements or any device that needs secure disposal should be returned to IT staff within the school or the Data Protection Lead in person.
- Media such as CDs or DVDs, which contain data and are no longer required will be physically destroyed by the IT Department/Data Protection Lead.
- 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.

(g) Paper and Manual Filing Systems

- Paper based (or any non-electronic) information will be assigned an owner. A risk assessment will identify the appropriate level of protection for the information being stored. Paper and files in the School will be protected by one of the following measures:
- Locked filing cabinets with restricted access to keys by appropriate staff only. Keys will be stored away from cabinets.
- Locked safes
- Stored in a secure area protected by access controls.
- Depending on the content of the sensitive data contained within papers and files, the appropriate member of staff will be responsible for the storing and protecting of the data in line with the secure filing system process.

(h) Security of Equipment and Documents Off School Premises

- Information storage equipment, such as computers, laptops, tablets, mobile phones and external storage devices will only be taken off school site if authorisation from the Head Teacher has been obtained.
- Personally identifiable information, sensitive or confidential data contained within paper-based documentation will only be taken off school site if authorisation from the Head Teacher has been obtained.
- Staff will adhere to the following security guidelines when taking equipment and/or documents off school site:
- Equipment/documents will not be left unattended in public places.
- Equipment/documents will not be left unattended in a vehicle unless the property is concealed from view and all doors are locked, windows and the roof closed and fastened, all security devices on the vehicle are put in full and effective operation and all keys/removable ignition devices removed from the vehicle.
- Equipment/documents will not be left open to theft or damage whether in school, during transit or at home.
- Where possible, equipment/documents will be stored discreetly (e.g., laptops should be carried in less formal bags)
- Equipment/documents will be returned to the school as soon as is practically possible.
- Data encryption will be in place, and manufacturer's instructions for protecting school equipment will be observed at all times.

(i) Physical Security

- This section is related to building security and the level of care that will be taken when transporting computers or paper files outside of the building.
- Data held by the school will be protected against the possibility that it could be stolen, lost or otherwise divulged by physical (or non-electronic) means. The following organisational security measures are in place to protect all sensitive, personally identifiable and confidential information:
- The school premises are protected by door locks and access codes. The codes remain secure and form part of the school's physical security procedures and as such help to keep personal, sensitive and confidential data safe.
- Doors and windows are locked when areas are left unattended and external doors (including loading bay/fire doors) are locked when not in use.
- All visitors sign in and receive a Visitor's Authentication Badge. This is issued by the staff in Reception and applies to all Visitors.
- All Visitors/Attendees will be supervised at all times and are required to wear visible authorised identification, and to record their date/time of entry/departure and person(s) being visited.
- Where personally identifiable, sensitive or confidential data is requested, staff will ensure it is a legitimate request and data is not breached. If in doubt, checks with the Data Protection Lead or the Data Protection Officer will be carried out.

(j) CCTV

- The school operates a CCTV system to monitor activities within and around school, to identify instances of criminal activity and to ensure the safety and wellbeing of the school community. The school do not need to ask the permission of individuals on the school site to record images on CCTV.
- The school will only operate overt surveillance and will display signs in the areas of the school where this is in operation. Covert surveillance (i.e., which is intentionally not shared with the individuals being recorded) is not condoned by the school.
- Any enquiries or complaints about the schools CCTV system should be directed towards the data protection lead in school (see point 8) in the first instance, who will investigate as required, and respond in accordance with the schools CCTV policy.
- For more details, please refer to the schools CCTV Policy

(k) Staff use of work devices

- Devices provided to staff are to be used for work purposes only. Staff will not save or access their personal data on school devices.
- Staff are aware that work email accounts and files may be accessed by the school if required to support management of the school e.g., in the case of staff absence or handover.

(l) Use of AI software

- The school recognise the benefits of AI tools in a work setting however staff are informed of the challenges and risks AI systems may pose.
- AI software within official or licensed software will be used appropriately and reasonably to accomplish tasks.
- If staff are planning to use a new AI system, staff will first inform the DPL and IT support of this intention. If applicable, informed staff will recommend alternative solutions that may offer a safer and more secure use of data. If alternatives are not known, staff may be asked to complete a risk assessment or data protection impact assessment prior to use.
- In the interest of mitigating risks of a data breach, staff will not input confidential or sensitive information into AI Chatbots (Copilot, ChatGPT, Gemini etc). Such information includes but is not limited to personal data (also referred to in GDPR as Personally Identifiable Information); commercially sensitive or confidential data; and credentials (e.g., passwords).

(7) Accountability: *the Controller will be able to demonstrate compliance with the previous principles.* The school will do this by employing measures including:

(a) Data Protection Officer and Data Protection Lead

- A Data Protection Officer (DPO) is appointed to the school who has suitable knowledge and experience to fulfil this role and has a direct line of report through to the Head Teacher and Governing body for data protection related matters.
- On a day-to-day basis, the first point of contact within the school is the Data Protection lead. The Data Protection lead will liaise with the Data Protection Officer for advice and guidance as required.

- The DPO will undertake periodic monitoring activities to help ensure compliance with the regulation. They will be informed of any suspected data breach, and will help to investigate circumstances surrounding breaches, and ascertain whether they are required to be reported to the ICO.
- The DPO will be informed of any Subject Access Requests that are submitted to the school and will assist in making the response to the Data Subject.
- For our school, the Data Protection Officer is provided to us by SIPS Education and are contactable via gdpr@sips.co.uk or 0121 296 3000.
- The schools Governing Body will be kept informed of the ongoing compliance via reports to the Full Governing Body which will include an overview of any data breaches that have occurred along with actions taken, and any Subject Access Requests received and responded to.

(b) Responsibilities

- Everyone in school is responsible for protecting personal data.
- Governors and trustees check that the school are monitoring their data protection performance, supporting the DPL and DPO, security measures are appropriate to keep data protected and cyber security is considered within the continuity plan.
- Senior leaders are responsible for deciding how school`s maintain security and how data is shared, setting policies for the use of data and technology, making sure contracts with third-party processors are relevant and supporting staff with annual staff training.
- All staff should be aware of their duties and processes for handling personal information and the procedures to respond to a data breach or subject access request.

(c) Staff and Governor Training

- Annual training for staff and governors is provided by either the DPO or Head Teacher/Data Protection Lead or via an eLearning training platform. In addition to this, regular reminders to staff on the content and expectations of this policy and the procedures to follow to safeguard personal data is carried out.

(d) Third Party Organisations

- Where the school needs to share personal data with third party organisations (Data Processors), it will ensure that adequate checks have been undertaken on the robustness of the processors data protection systems to safeguard the information shared and will maintain a written record of this.

(e) Data Protection Impact Assessment

- Data Protection will be considered as part of all project planning when the school are reviewing systems for data collection and data processing. Where required, the school will undertake Data Protection Impact Assessments to ensure appropriate measures are put in place to safeguard the data, prevent breaches and ensure compliance with the requirements of the Regulation.

Photographs and Videos

The school may take photographs and videos of individuals as part of school activities. Such images may be used for:

- Notice boards around school, school newsletters, brochures etc
- External agencies such as the school photographer, newspapers/media campaigns
- School website or social media

In order to do this, we will obtain written consent from parents / carers before we take photographs or videos of your child. We will do this yearly and upon induction to the school. When we seek your consent, we will clearly explain how the photographs and/or videos are to be used.

You have the right to withdraw consent at any time, upon which we will delete any images already taken and we will not distribute those images further.

As part of our 'public task,' we may take a photograph of your child without requesting consent from you. This would be in circumstances where identification of a child with an existing medical condition/allergy is required to meet the needs of your child and to keep them safe.

Where photographs and/or videos are taken by parents / carers at school events for their own personal use, the requirements of data protection legislation do not apply. However, we do ask that should your photos / videos capture images of other pupils in addition to their own child, that these are not shared in any public way (including on social media sites) for safeguarding reasons unless all relevant parents / carers have given their consent for them to do so.

Data Security and Storage of Data

All devices used in school and provided to staff including mobile phone, laptop, memory stick, tablet, external hard drive, computer etc, will be encrypted. Care will be taken to safeguard the equipment against loss or damage. Passwords used on all devices to encrypt information, will not be shared or written down.

All devices provided by the school will only be used for the purposes for which they were supplied.

Memory sticks that do not require a password to access the data contained on it will not be used and are not permitted by the school.

Any storage devices no longer required, which may contain information that is surplus to requirements, or any device will be disposed of securely.

Media such as CDs or DVDs, which contain data and no longer required will be physically destroyed.

Paper based documents and files containing personal data, which is stored in School will be protected by one of the following measures:

- Locked filing cabinets with restricted access to keys by appropriate staff only. Keys will be stored away from cabinets.
- Locked safes
- Stored in a secure area protected by access controls.

Depending on the content of the sensitive data contained within papers-based documents and files, an appropriate member of staff will be responsible for the storing and protecting of the data in line with the secure filing system process.

Subject Access Requests

Individuals (Data Subjects) have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed.
- Access to a copy of the data
- The purpose 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 is not possible, the criteria used to determine this period.
- Where relevant, the existence of the right to request rectification, erasure or restrictions, or to object to such processing.
- The right to lodge a complaint with the ICO or another supervisory authority.
- The source of the data, if not the individual
- The safeguards provided if the data is being transferred internationally.

It is important to bear in mind that a child's personal data is just that – their data – and does not belong to their parent / carer. As such, if a parent or carer wishes to make a subject access request for data relating to their child, the pupil will need to have given their consent depending on their age and level of understanding.

The age of 13 is used as a guide to determine when a child is generally likely to be mature enough to understand their rights, and accordingly any requests for their personal data from this age onwards would generally be expected to come from the child themselves.

For children below this age, it is less likely that they will fully understand the implications of a SAR, and so it would normally be acceptable for the request to come from the parent / carer.

Both above situations are used as a guide only, and each request (and requestor) will be assessed on an individual case by case basis.

Subject access requests can be submitted in any form to any member of staff within the school. However, the school may contact the requester for more details in order for the school to respond to requests appropriately. If staff receive a subject access request in any form, they will forward to the data protection lead within the school immediately. The data

protection officer will also be advised to ensure appropriate support is provided to the school to fulfil the request.

Parents and staff can also contact the data protection lead within the school to make a subject access request via email to office@st-martins.sandwell.sch.uk.

Information about how to make a Subject Access Request or for more details can be obtained from the Data Protection Lead within the school.

(a) Responding to a Subject Access Request

When responding to requests, the school may:

- contact the individual via telephone to confirm the request has been made by them.
- ask the individual to provide further details so that the school can verify and confirm the data required.
- request 2 forms of identification of the individual. Proof of address will also be verified.
- If a third party is requesting data, written authority or a power of attorney will be verified.

Requests will be responded to within 1 calendar month from receipt of the request. If the 30th day falls on a weekend or bank holiday, the pack will be made available on the next working day. However, if additional information is required for the school to fulfil the request, the response period will be from receipt of all information obtained. This includes receipt of proof of identity and proof of address where relevant.

While conducting searches for data, if, during this process, the school require further information from the requester, the response period may be paused as they await a response to allow them to continue the process, altering the deadline.

The response to the Subject Access Request will be made in the same format as the request was received unless the preferred format has been included in the request. For example, if the request is made by email, the data will be received electronically.

Based on the complexity of the request and in line with Article 12 (3) GDPR, the timeframe in which to respond to a Subject Access Request may be extended up to 3 calendar months if required. In such instances the school will liaise with the Data Protection Officer and liaise with the requester to advise of the response time or any delays at the earliest opportunity.

Data provided to the requester may contain details of other individuals and therefore such data will be redacted (blanked out) to protect those individuals' identity and personal data. Details contained within the documents will pertain to the appropriate individual only.

When responding to the request, the school may decide against disclosing information for a variety of reasons, including if it;

- would have an adverse effect on the rights and freedom of others.
- includes information that might cause serious harm to the physical or mental health of the pupil or another individual;

- includes information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests;
- includes information contained in adoption and parental order records;
- includes certain information which may be used in legal proceedings;
- would include personal data relating to another individual, where; the school cannot sufficiently anonymise the data to protect that individual's rights,' we do not have their consent to release that individuals' data, and it would be unreasonable to proceed without such consent.
- Safeguarding information recorded on safeguarding systems if release of the data could have the potential to cause serious harm to an individual or a live, legal process.

The school are required to conduct reasonable and proportionate searches to fulfil a request. If a request is determined to be 'excessive or vexatious' the school has the right to refuse the request, or in some cases, charge a reasonable fee to cover the administrative costs of responding to the request.

If the school refuses a request, they will inform the individual of the reasons why and advise them of their right to complain to the ICO, if they wish to do so.

Data Breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches. The school has robust procedures in place to deal with any personal data breach and will notify the ICO where we are legally required to do so. Data subjects will be notified in instances where the rights and freedoms of such individuals has been compromised. The school will work with their Data Protection Officer to address a breach and school processes will be reviewed to mitigate risks if it is appropriate to do so.

(a) Responding to Data Breaches

If any member of staff becomes aware of a data breach situation, they will ensure this is reported to the Data Protection Lead as soon as possible. The school will keep a record of all breaches and investigate them to an appropriate level, to ascertain what can be learnt from the circumstances surrounding each. Upon completion of an investigation procedures will be reviewed as required with the aim of preventing a similar breach occurring again.

Some breaches of a more serious nature will need to be reported to the ICO. The DPO will help the school to ascertain whether a breach is reportable and will advise on all such occasions if this is the case. The Data Protection Lead will liaise with the DPO to determine whether a breach is reportable to the ICO.

Where breaches are reportable, the school is legally required to submit the report to the ICO within 72 hours of the school becoming aware of the breach, and therefore staff members must advise the Data Protection Lead as soon as a breach is realised.

A near miss will also be reported to the DPL so that the school can learn from these and use them as a way of informing future revisions to our policies and/or procedures for data protection.

Contact Details

In the first instance concerns, questions or complaints should be directed to the Data Protection Lead at *office@st-martins.sandwell.sch.uk* . This includes if a data subject wishes to make a Subject Access Request, is concerned about a data breach or has general queries in relation to data protection within the school.

If a data subject requires further assistance after contacting the Data Protection Lead, this should then be discussed with the Data Protection Officer who can be contacted at:

Email: gdpr@sips.co.uk

Telephone number: 0121 296 3000.

After contacting the Data Protection Lead and Data Protection Officer, if a data subject remains dissatisfied with the assistance that they have received, they can make a formal complaint to the Information Commissioners Office.

The Information Commissioner can be contacted at:
Information Commissioners Office, Wycliffe House Water Lane Wilmslow Cheshire, SK9 5AF
Tel: 0303 123 1113
Website: https://ico.org.uk

For more information about the complaints process, please see our *Data Protection Complaints Policy.*