Data Protection Policy For School Staff

The Westminster School

Version 2

Date of last review:	May 2020
Date of this review:	July 2022
Date of next review:	July 2024

1. Introduction – What is GDPR?

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. This policy has been put into place to ensure all staff and Governors in the school have an understanding of 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.

2. Applicability

This policy will apply to any member of staff in the school who process personally identifiable information. Such individuals must ensure that they are familiar with the contents and behaviours identified within this policy, and should ensure they refer to this policy when carrying out their duties.

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).

3. 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.
- ***Special Categories of Personal Data*** – personal data which is more sensitive and so needs more protection, including information about an individuals, 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.
- ***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 the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data.
- ***ICO*** – Information Commissioners Office (Supervising Authority in the UK)

4. Principles

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 all staff employed by our school, and to external organisations or individual's working on our behalf comply with the principles on a day to day basis.

4.1 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.

Data Mapping

In order to do this, the school will undertake a data mapping exercise to identify and record those data sets / records held within the school, which contain personal information, and in each case, record the lawful basis for processing. Without a lawful basis, processing must not take place, and the personal data should not be held by the school.

The data mapping document will be held by the School Business Manager and should be considered to be a 'live' document. All staff will be asked periodically to assist in reviewing 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 in each occasion.

Privacy Notices

The school will ensure all Data Subjects are clear about the ways in which the school is processing their personal data. This will include publishing a privacy notice, which provides details of what personally identifiable information is held by the school, how it will be processed, stored, the organisations it will be shared with, the lawful basis for processing and how long the data will be held prior to destruction. The Data Mapping document will be used as the source of information, to populate the Privacy Notices.

The Privacy Notice will be made readily available as follows:

Pupils, Parents and Carers – Privacy notice will be located on the school's website.

Staff, volunteers, governors – Privacy notice will be located on the School Policies Hub.

Visitors and Contractors – Privacy notice will be located on the school's website.

4.2 Purpose Limitation and Minimisation: *personal data should be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.*

Internal records will be maintained to reflect the purposes for which processing of data will take place. More specifically, this will be included on the data mapping record, and will include:

- a record of the purpose (the lawful basis)
- description of the categories of individuals and the personal data held
- the categories of recipients of the data (e.g. Third party organisations who the school shares the data with)
- the location of the data – where it is stored.
- retention schedules for the personal data.

Appropriate technical and organisational measures that must be maintained, in order to safeguard personal data are identified in this policy in general. They will be further documented within Data Privacy Impact Assessments, if the processing of personal data is higher risk and could result in a risk to the rights and freedoms of the individual (see section 4.6 - Accountability, for further information on Data Privacy Impact Assessments).

Minimisation: *the personal data must be 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'*

The school will periodically review its' data capture forms and processes, to ensure that the information being requested is not excessive, and that the school is not capturing more personal information than is required.

Personal data collected by members of staff will, wherever possible, be limited to the scope of what is laid out in official school data capture forms. If a member of staff wishes to introduce the use of new technology that captures personally identifiable information, including apps used in classrooms they will first speak with the data protection lead in school Angela Gibson/Lance Goodby. The DPL will ensure appropriate measures, including consents (as required) are in place, and the data mapping document is 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 Officer for further guidance.

4.3 **Accuracy**: *every reasonable step must 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*

The school shall take proactive steps to check the accuracy of information held within its systems and will subsequently carry out updates as required, through a variety of measures. These include, but are not limited to:

- 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 parents evenings
- Termly newsletters to remind parents to update their data if required.
- Checking the accuracy of data during contact with parents including first day calling conversation via SENCO etc.
- Checking accuracy of staff details via email reminders to update details

4.4 **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 the various records held in the school containing personal data, will be identified and documented as part of the data mapping activity.

The school will refer to the Information Records Management Society (IRMS) Toolkit as its' guide when determining the appropriate retention periods for documents. A copy of this toolkit is available to staff via www.irms.org.uk .

Destruction of Records

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.

The school will shred paper-based records, and overwrite or delete electronic files. School may also use a third party to safely dispose of records on the schools 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: *Archived documents are stored off site. School uses a secure shredding service agency and also shreds documents in-house.*

4.5 **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*

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 Angela Gibson or Lance Goodby in the first instance, who will liaise with the Data Protection Officer if required.

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 characters long, have a mixture of upper case and lower case letters, at least one number and one character.

Passwords will be changed regularly, and never 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.

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 Acceptable Use Policy.

Staff will follow the secure process of accessing data via a secure function 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.

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 Angela Gibson/Lance Goodby.

- 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.

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.
- Personal devices such as mobile phones, tablets, laptops or any device that can contain personally identifiable information will not be used and is not permitted by the school.
- 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 is in need of 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.

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.

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.

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 Name or the Data Protection Officer will be carried out.

CCTV

The school operates a CCTV system to monitor activities within and around school, to identify instances of criminal activity and in order 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 N 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

4.6 **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 (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 who 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@sipseducation.co.uk or 0121 296 3000.

The school's Governing Body will be kept informed of the ongoing compliance via reports to Governing Board meetings 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.

Staff and Governor Training –

Annual training for staff and governors is provided 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.

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 in order to safeguard the information shared, and will maintain a written record of this.

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.

5. 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. 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.

Subject Access Requests

Parents, carers, students (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 isn't 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

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 dependent on their age and level of understanding.

The age of 13 is used as a guide todetermine 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 SARs, and so it would normally be acceptable for the request to come from the parent / carer.

Both of the 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 .

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

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. However, if additional information is required in order 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.

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.

  If a request is determined to be 'excessive or vextious' 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.

6. 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.

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, in order 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.

7. Complaints to the Information Commissioner

Should individuals be dissatisfied with the way the school has handled a request and want to make a complaint, they may write to the Information Commissioner, who is an independent regulator. Any complaint to the Information Commissioner is without prejudice to their right to seek redress through the courts.

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

8. Contact Details

If a data subject wishes to make a Subject Access Request (see point 5) or have general queries in relation to data protection within school, these should be directed to the Data Protection Lead within the school.

In the first instance concerns, questions or complaints, can be discussed with the Data Protection Officer at gdpr@sips.co.uk or telephone number 0121 296 3000. This would include situations where there are concerns about the way a Subject Access Request or a data breach has been addressed or the robustness of policy or procedures within school in relation to Data Protection.

If a data subject remains dissatisfied with the assistance that they have received or if they do not feel their subject access request has been dealt with appropriately or they have concerns with regards to a possible breach they can make a formal complaint to the Information Commissioners Office. This can be done via the website at www.ico.org.uk. Telephone: 0303 123 1113 or in writing to Information Commissioners Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5A