Temple Meadow Primary School

Temple Meadow Primary School

Growing together, learning together

General Data Protection Regulations Policy

Safeguarding Policy Statement

This policy is part of the wider umbrella of Keeping Children Safe in Education - and Temple Meadow's Safeguarding and Child Protection Policy.

Policy Ownership: SBM/HT

To SLT:	July 2023
To Staff:	July 2023
To Governors:	July 2023
Document Live date:	July 2023
Next Review Date:	**July 2024**

Contents

1. **Introduction – what is GDPR?**

The General Data Protection Regulation replaces the Data Protection Act 1998, as of 25th May 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 out 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 performing 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.

Legality, Transparency and Fairness.

The school will only process personal data, where it is able to demonstrate that it has a 'Lawful basis' for the processing activity. In order to do this, the school will undertake a data audit to identify and document those data sets / records held within the school, which contain personal information, and in each case, document 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 audit will be held by the **DPL (SBM)** and should be considered to be a 'live' document. All staff may be asked periodically to assist in reviewing the data audit to ensure all data sets currently in use within the school have been captured and considered, and a lawful basis for processing identified on each occasion.

The school will endeavour to ensure all Data Subjects are clear about the ways in which the school is processing its personal data. This will include publishing information on the type of personal data being collected, the lawful basis for processing, and types of other organisations who the information is shared with, within a privacy notice.

The Privacy Notice will be made readily available by posting this on the school website at Temple Meadow Primary School - Policies. Paper based copies are also available from the school office.

4.1 **Purpose Limitation:** ***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 will take place. More specifically, this will be included on the data audit record, and will include a record of the purpose, 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.

Appropriate technical and organisational measures that must be maintained in order to safeguard personal data, are identified in this policy. Where personal data presents a higher risk, additional measures will be documented in a Data Protection Impact Assessment (see Appendix 1 for further information on Data Impact Assessments).

4.2 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 such as dojo, tapestry etc, they will first speak with the data protection lead in school; Mr James Maton-Collingbourne (SBM). The DPL will ensure appropriate measures, including consents (as required) are in place, and the data mapping document is updated accordingly.

Personal data collected by members of staff should, wherever possible, be limited to the scope of what is laid out in official school data capture forms. Wherever there is any uncertainty about the level of information being requested from Data Subjects, a referral should be made to the DPO for further guidance.

4.3 **Accuracy:** ***every reasonable step must be taken to ensure that personal data that are 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 to subsequently conduct 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 medical details of pupils**
- **Use of apps such as ParentLite to allow parents real-time access to update the above data on SIMS**
- **Checking attainment data in systems on a regular basis, through the use of pupil progress meetings**
- **Checking accuracy of staff details through issuing data collection forms to all staff on an annual basis, as well as facilitating staff access to key personal information through a self-service HR portal.**

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 audit activity.

The school uses the **Information Records Management Society Toolkit** as its' guide when determining the appropriate retention periods for documents. A copy of this toolkit is available to staff on the **School Network S Drive**

Document Archiving

Paper based documents which reach the end of their usable life enter a retention cycle (refer to Archive & Retention Policy), are securely stored in the Archive storage facility, located on the Wright's Lane car park. All documents are stored in clearly labelled boxes, stating their archiving date and scheduled disposal date.

Paper Document Destruction

In order to ensure the secure disposal of all paper documents, the school has entered into a secure waste transfer contract with 'Shred Pro Ltd'. There are seven paper waste disposal consoles strategically cited on the school site in order to provide complete coverage of secure paper disposal. The consoles are emptied on a four-weekly cycle. Shredding bags are also available in school for surplus paper waste, which can be collated and securely stored in the archive storage facility, until the next scheduled waste collection occurs. The locations of the seven consoles are specified below:

Console Location	Intended users (although not limited to)
School Office	Office Team & HT
Junior Corridor	Y6, DHT & Ricoh Junior waste
Dining Hall	Y4 & Y5
Pastoral Office	PSK Team
Clifton Building	Y3 & Ricoh Clifton waste
Infant Corridor	Y1, Y2 & Ricoh Infant waste
Early Years Café	EYFS

Electronic Document Destruction

Electronic documents are retained in conjunction with the Archive and Retention Policy. The school periodically conducts a sweep of data held on the school website in order to ensure no information is stored beyond its expiry

date. The Archiving facility within the SIMS MIS system is also available to archive data, in conjunction with the stated archive and retention strategy.

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 should not be left unlocked when workstations are left unattended. PCs can be locked by hitting the windows and L keys or Ctrl-Alt-Delete.

- Any paper-based documents containing personal information should be secured at the end of the day, and when rooms / offices are left unattended. 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 should in the first instance speak with the **SBM** who will consult with the DPO if required.

- Positioning of computer screens should be considered carefully 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. Privacy screens will be considered where positioning of screens alone will not address this concern.

- Passwords and protection of hardware. Passwords for accessing systems must be complex enough to make it extremely difficult for third parties to break them: passwords should be at least eight characters long, have a mixture of upper case and lower-case letters, at least one number. The school network dictates that users change passwords annually. **Passwords should never be shared with any other staff members**.

- School mobile devices (Staff Laptops/Tablets) must be protected to the same high standard. The school network dictates that a password/PIN (as applicable) must be registered prior to use, in line with the school's network security policy. Assigned device owners are personally responsible for any information accessed or disclosed on these devices, **so it is imperative that staff keep passwords/PINS safe and secure, and do not share it with anyone else.**

Accessing information remotely

- Staff members accessing information away from school should only use the Office 365 SharePoint facility to access, edit and save documents. Documents should not be downloaded and or saved to personal devices, inc. laptops/tablets. If a document is inadvertently saved to a personal device, it should be deleted immediately. The SharePoint facility also enables the secure transfer of documents back into school. **USB Memory sticks/portable hard drives are not permitted to be used in school, or to transfer any school documents.**
- School email accounts can only be accessed via a school device or over a web browser, enabling access to Office 365. This strategy ensures that school specified device encryption, and or password protection applied through Office 365 protects all stored data on email accounts. **Staff are not permitted to install school email accounts on to apps on personal devices.**
- If accessing documents attached to emails on personal devices, staff should take extra care when considering downloading attachments. As appose to just viewing a document, if the decision is taken to download; potentially sensitive information is stored on a personal device. **Staff should therefore avoid downloading documents in this circumstance, unless they can be 100% confident that the document will be permanently deleted after use.** Downloading documents in this circumstance to a school device is however permitted.

Sharing information with others

Inside the School:

- When sharing information with others within the school, if information is of a confidential, sensitive or personal nature, it must be treated as such. Information should only be shared with the individuals who require it, do not copy people into emails if they do not require access to the information contained within. Delete sensitive, confidential, or personal information once it has been used for the purpose it has been collected and is no longer required.
- When identifying pupils in public spaces, **only first names or initials will be used**
- When identifying pupils in classroom spaces, **first name and surname may be used, in accordance with management discretion**

Outside the School:

Where more than one piece of personal, sensitive or confidential data is to be sent, one of several methods can be used. If in doubt, please check with the **DPL (SBM)**.

- Secure transmission: Where possible, use recognised secure transmission methods such as MoveIt.

- Never send personal/sensitive data within the body of an email. If email is the only method of transmission available, ensure the information is attached in a password protected document. The password must be agreed with the email recipient in advance, and via telephone, not in another email. Never include the password in the email to which the password protected document is attached, nor send the password via another email (if the first email is intercepted, then the second could also be).

- Ensure that the request for data is a valid one and that only the required data is provided. Always check why people require the data they ask for – if in doubt check with the SBM before sending.

- Make sure that the data is up to date. Check the accuracy of the data before sending.

- School Emails should never be sent to public email addresses (e.g. Hotmail, Gmail etc.), unless this has been clearly identified by the recipient as their business email address.

- When sending emails to individuals outside of the organisation, and including internal colleagues; always use Bcc not Cc. This will ensure that internal colleague details/contact information are not inadvertently disclosed to third parties.

When sending information (including letters) via post the following must be adhered to:

- Always get a second person to check the address is correct before sending. Pay particular attention to numbers as these are easily transposed, however, be aware the responsibility for the accuracy is still with the Sender not the Checker
- Always use window envelopes if the address is pre-populated on the enclosed letter to avoid transcription errors or typed labels to avoid issues in relation to legibility of handwriting.
- Always ensure that envelopes are securely sealed. Use additional methods such as sticky tape, glue or staples if deemed necessary
- Double check that no additional information has been included that is not relevant e.g. something mistakenly attached. Only send relevant data. Check that it is valid and accurate and no additional information i.e. additional sheets are included in error.
- If a request is received from an outside agency such as the Police, this should be referred in the first instance to the **Headteacher**

Paper Filing Systems

The security of paper based (or any non-electronic) information is managed through the proactive use of a corresponding risk assessment. Refer to the Paper Filing System risk assessment for strategies adopted in safeguarding the integrity of all based documents.

Security of Equipment and Documents Off-Premises

School documents/files containing personal, sensitive or confidential data should only be taken offsite for essential use, by staff who are authorised to do so.

The following security guidelines must be adhered to for all equipment and documents taken offsite, it must:

- not be left unattended in public places.
- 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
- not be left open to theft or damage whether in the office, during transit or at home
- where possible, be disguised (e.g. laptops should be carried in less formal bags)
- be returned to the school as soon as is possible.
- Where it is necessary to transport sensitive or personal data in this manner, data encryption must be in place, and manufacturer's instructions for protecting the equipment should be observed at all times

Physical Security

Our data must be protected against the possibility that it could be stolen, lost or otherwise divulged by physical (or non-electronic) means. This section is related to building security and the level of care that you are expected to provide when transporting computers or paper files outside of the building.

- Our premises are protected by magnetic door locks and access codes. It is important that the codes remain secure as these form part of our physical security procedures and as such help to keep our personal, sensitive and confidential data safe.
- Doors and windows must be locked when unattended and external doors (including loading bay/fire doors) must be locked when not in use.
- All visitors must sign in and receive a Visitor's Authentication Badge. This is issued by the staff in the School Office and applies to all Visitors.
- All Visitors/Attendees should 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.
- Some visitors may require access to confidential data or computer systems that contain such data. If such access is requested, it is the employee's responsibility to ensure it is a legitimate request and data protection is not breached. If in doubt, please check with the **DPL (SBM)** or the DPO.

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

Ensuring a DPO is appointed. This individual will have suitable knowledge and experience to fulfil this role and will have 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 **(DPL SBM)**; the DPL will consult with the DPO for advice and guidance as required.

The DPO will undertake periodic monitoring activities to help ensure compliance with the regulation. They must 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 must also 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 DPO is provided to us by **SIPS Education, and are contactable via gdpr@sipseducation or 0121 296 3000.**

Our Governing Body will be kept informed of our 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.

Training for staff and Governors will be provided by the DPO on an annual basis, and further supplemented by reminders in school on policy and procedures, issued by the SBM via the SLT newsletter

Where the school needs to share personal data with third party organisations (Data Processors), it will ensure that adequate steps have been taken to vet the robustness of the Processors systems in order to safeguard the information shared and will maintain a written record of this.

Data Protection will be considered as part of all project planning when we are reviewing our systems for data collection and data processing. Where required, we 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. A copy of the Data Protection Impact Assessment is included at Appendix A.

5. The rights of the Data Subject

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 consult 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 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

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 thirteen is used as a guide to determine when a child is likely to be mature enough to understand their rights, and accordingly any requests for their personal data from this age onwards would 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 by emailing tm.admin@meadow.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; Mr James Maton-Collingbourne (SBM).

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 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 one 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 time in which to respond to a Subject Access Request may be extended up to three calendar months if required. In such instances the school will consult with the Data Protection Officer and consult 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 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.

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 consult 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; Mr James Maton-Collingbourne (SBM).

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 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

Appendices

Appendix 1: Data Protection Impact Assessment Template

Data – Electronic or Hard Copy	Current Process	Impact of threat if occurs: 1 = low 5 = High	Likelihood: Low, Medium, High	Steps Taken to Minimise Risk	Action Plan/Next Steps	Review Date