St Michael & All Angels primary School

Data Protection Policy

Version:	1-5
Ratified by:	Governors
Date ratified:	September 2025
Name of organisation/author:	SMAAA
Name of responsible committee/individual:	Maria Graham
Date issued:	3/09/25
Review date:	3/09/26
Target audience:	All employees

1. Introduction

1.1 This policy provides a framework for ensuring that St Michael & All Angels Primary School meets it's obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). The legislation tells organisations how to manage personal data that they hold, giving principles and rights that must be upheld. The UK GDPR and the DPA 2018 encourages a balance between the individual's right to privacy and an organisation's need to conduct legitimate and appropriate operations with personal data.

1.2 St Michael & All Angels Primary School is committed to protecting the privacy of individuals and handles all personal data in a manner that complies with the UK GDPR and DPA 2018. The school has established the following policy to support this commitment. It is the **personal responsibility** of all employees (temporary or permanent), Governors, contractors, agents, volunteers and anyone else using personal data on the school's behalf to comply with this policy.

1.3 This policy explains what our expectations are when processing personal information. This policy should be read together with the Information Security Acceptable Use Policy, and the School Records Retention and Disposal Schedule.

2. The Data Protection Principles and Definitions

2.1 The UK GDPR and DPA 2018 is concerned with the use (processing) of personal data.

Personal data is information that either on its own, or when combined with other information, can be used to identify a living individual.

Examples of personal data include: - names, addresses, dates of birth, photographs, IP Addresses, Vehicle Registration Plates, CCTV footage.

The UK GDPR also defines personal data that is more sensitive and must be treated with a higher level of privacy and respect. This is called Special Category Data.

Special Category Data is any data that falls into the following categories: - racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data such as fingerprints, sex history or sexual orientation, any data relating to physical or mental health conditions.

Processing Data This means any use of the personal data. This includes collecting, disclosing, destroying, archiving and organising.

Data Subject is the person who the personal data is about. For example, pupils, parents, staff, and Governors, would be considered data subjects as their personal details are held on school systems and hardcopy documents.
Data Controller is usually an organisation who dictates the reason and purpose for how personal data is processed. The school itself is a Data Controller as it chooses how it collects, uses and shares the personal data that it processes. The school is registered as a Data Controller with the Information Commissioner's Office registration number Z9055033

The Information Commissioner's Office (ICO) is the regulator for data protection and privacy law in the England, Wales, and Northern Ireland. They have the power to take enforcement action against organisations for breaches of the DPA18 or the UK GDPR.

2.2 The Principles

The UK GDPR contains a number of key principles that must be met in order to use personal data in line with the law.

Personal Data must be: -

1. Processed fairly, lawfully and transparently
2. Processed for a specified and legitimate purpose
3. Adequate, relevant and limited to what is relevant
4. Accurate and up to date
5. Kept for no longer than is necessary
6. Stored securely using technical and organisational measures

Principle One – Fair, Lawful and Transparent

Fair and Transparent

When the School collects personal data from an individual, we must tell them of what we intend to do with data once we have it.

We use a Privacy Notice to inform people about how we use their personal data.

The Privacy Notice must include information such as – what the personal data will be used for, who it will be shared with and how long it will be kept for.

The Privacy Notice must be provided to the data subject as soon as possible when processing their personal information and this can be done online via the school website, through the post, or in the form of a recorded voice message. As long as the Privacy Notice is provided, it can take any form necessary.

The school Privacy Notice can be found on the school website here: www.smaaa.info

Lawful

To use personal data lawfully, the school must ensure that no laws are broken when we use the data. This means we cannot use data to break any other laws within the UK.

As well as this, the school must meet what is called a lawful basis for processing when processing the personal information. The lawful bases for processing are explained below. There are six of them and are all equally valid.

The school can use personal data if we meet one of the following lawful bases from UK GDPR Article 6:-

- The data subject has consented to their information being used. This consent must be specific, informed and freely given. The data subject must know what they are consenting to and be given a genuine choice, before consent can be classed as appropriately obtained. Generally, schools use consent for the purpose of photography and video recordings that they are going to share through their social media channels, printed publications (e.g., a prospectus) or via their website. The school will ensure that the school consent form is used when seeking to gain consent and a record of consent is maintained.
- The personal data is being used to perform a contract with the data subject or to undertake actions necessary for creating a contract with the data subject.
- The personal data has to be processed because legislation says that the school has to. This also applies when the school receives a court order that demands disclosure of information.
- The personal data is used in line with the vital interests of the data subject. This would be used to share personal data in the event of an emergency.
- The personal data is used in line with a public function (task) or legal power that the school.is meeting. For example, Section 537A of the Education Act 1996 places a statutory requirement on the school to submit a school census, including a set of named pupil records This power also allows the school to use information to complete this function. The school will use this lawful basis for the majority of their processing.
- The personal data is used in the legitimate interests of the school and does not conflict with the rights and freedoms of the data subject. When using this condition, it is best to consult with the Data Protection Officer. Schools can use this lawful basis for any processing that they are undertaking in pursuance of a legal obligation or a public task.

When we use Special Category (sensitive) personal data or criminal conviction data, we must identify an additional condition from UK GDPR, however, the majority of data will be processed under the following conditions:.

- The data subject has given explicit consent.
- Processing is necessary for the purposes of employment and social security and social protection law (if authorised by law).
- Processing is necessary to protect the vital interests of the data subject or of another natural person.
- Processing relates to personal data which are manifestly made public by the data subject.
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
- Processing is necessary for reasons of substantial public interest, (with a basis in law).
- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the

provision of health or social care or treatment or the management of health or social care systems and services (with a basis in law).
- Processing is necessary for reasons of public interest in the area of public health.

A number of the lawful bases listed above have additional requirements and the Data Protection Officer for the school can advise on this.

For several of the lawful bases used to process Special Category personal data the school must identify an additional lawful condition from the DPA18. The school Data Protection Officer will be able to provide advice and guidance regarding this.

Principle 2 – Specified and Legitimate Purpose

The school must only process personal data for a specified and legitimate purpose. This purpose must be in line with the school's aims and values and not contradict any laws or moral obligations.

Once we have collected personal data for a specific purpose, we must only use that personal data for purposes compatible with the original aim.

For example, if the school collects information regarding after school activities, we can use it for other after school activity purposes such as evaluating the quality of the service provided. However, we couldn't use after school activity information to inform school trip planning/school meal planning, as this is not a compatible purpose because it so different to the original purpose for collecting the information.

Principle 3 – Adequate, Relevant and limited to what is necessary

The school must only use, collect or share the personal data that we need in order to complete the purpose we are trying to achieve.

For example, if the school only needs to collect a name and address in order to complete the purpose, only the name and address should be collected.

Principle 4 – Accurate and up to date

The school must ensure that all of its information is as accurate as possible. This means that if we find out something new about a data subject such as a change of address, school systems are updated as soon as possible to reflect this change.

Inaccurate personal data can lead to breaches, such as letters or emails being sent to incorrect recipients or incorrect decisions being made about pupils, parents, staff and other stakeholders.

Principle 5 – Kept No Longer Than Necessary

The school has a responsibility to ensure that personal data is not retained for longer than necessary for the purposes for which the data is processed. The school has a Records Management Policy/Retention Schedule, which details how long we hold information for, this can be accessed from the school office.

Principle 6 – Stored Securely

The school must take all appropriate technical and organisational measures to keep information secure and prevent it from being lost or put at risk of being seen by people who shouldn't have access to it.

This can take a variety of forms. Some examples of appropriate technical and organisational measures can be found below.

Technical Measures

- Firewalls.
- Anti-virus software.
- Encryption.
- Use of secure email gateways such as Egress and Transport Layered Security (TLS).
- Virtual Private Networks (VPNs).
- Tiered access on systems.
- Locked cupboards or pedestals in locked offices.

Organisational Measures

- Policies and procedures in place to help staff understand their duties regarding data protection and information security.
- Annual data protection training for staff.
- Data Protection Impact Assessments (DPIA), which help to identify and mitigate risks relating to the processing of personal data.
- A more knowledgeable and open culture towards data protection

The aim of employing appropriate technical and organisational measures is to help staff use and retain personal information securely. This is by giving them the technology and the knowledge to know how to safely handle information. In line with this, if you identify any further training or equipment needs for your team, contact your line manager so that this can be arranged.

3. Access and use of personal data

3.1 Access and use of personal data held by the school is only permitted to employees (temporary and permanent), Governors, contractors, agents and anyone delegated access as part of their official duties.

School information is held on a need-to-know basis, meaning that unauthorised or inappropriate use of the information is strictly forbidden.

School employees and, where applicable, Governors, must only access personal data that they have a professional and legitimate need to see. Just because an employee has access to a specific system does not mean that the employee has the right to access all records within that system.

Any deliberate or malicious access to systems or records will be dealt with in line with the school's Disciplinary Procedures. There are also a range of criminal offences under the Computer Misuse Act 1990 and the DPA18 for unauthorised use, or destruction of personal data. These offences can be punished by up to 12 months in prison or a fine of up to £1,000.

More information about how to handle personal data can be found in the Acceptable Use Policy which may be found on the school website www.smaaa.info

Staff have an individual responsibility for the way handle personal data as part of their day to day work. As a school employee, they are required to keep all information you use secure and confidential.

The general rule when using personal data is, treat it with the respect that you expect your own personal data to be treated. All staff must ensure that their use of personal data is appropriate and respectful.

Staff Tips for using Personal Data

Handling and using personal data in line with the law is not complicated. The following tips are easy to follow, easy to implement and could make all the difference to your daily work in helping to avoid data breaches.

- Always lock your screen when you leave your desk. This avoids leaving your systems open to access and also stops those nearby reading any personal data you may have left onscreen.
- Clear documents away at the end of the day or when leaving your desk. This stops people who are walking past your desk from reading things they should not have access to.
- Always check for ID when holding doors open for people. It is everyone's responsibility to ensure the security of school buildings and make sure only authorised staff have access to them.
- Double check when entering information into school systems. Processing Inaccurate information is the biggest cause of school data breaches. Taking the time to check addresses and phone numbers is a vital part of data handling.
- Double check addresses when sending emails. It is easy to mistype or click the wrong name on Outlook. Take the time to get the recipient right and complete thorough checks before you press send.
- When taking information out of the office, think about the most appropriate way to do so. school tablets and laptops are encrypted and difficult to access if they are lost. Paper documents are not as secure as they can be read by anyone who finds them.
- If you don't need to print something, don't.
- If you are regularly sending personal information to organisations outside of the school, ensure you have a TLS connection in place with the external email or a secure email gateway, such as Egress. Guidance for Egress and TLS is available on BERTHA. If you do not have encrypted email the personal data must be contained in password protected/encrypted document that

is attached to the email. Personal information must not be disclosed in the body of the email. The password to access the documents must only be disclosed to the recipient following confirmation of receipt and must be via an alternative method (e.g. phone call). It is recommended that when contacting the third party to confirm the password that the contact number is sourced via 118 or a Google check.

- Take care when working from home. Your family members don't have a right to see the information you use for work.
- Don't leave equipment or documents in your car overnight if you need to take them home. When in transit staff must ensure that their laptop and documents containing personal information and school proprietary are placed out of site (e.g. in the boot).

Using School Systems

- Just because you have access to a system, this does not mean you have the right to access all of the information on it. Access is on a "need to know" basis.
- "Curiosity" checks are not permitted. You must have a genuine, legitimate work purpose to access information
- Never share passwords. If a colleague forgets their password, they need to have it reset by IT. Do not let them access a system under your username.
- Any information you access on a system will be logged. Do not let colleagues use your computer to retrieve information and do not undertake requests on their behalf.
- Always be professional when using School systems. Do not input anything derogatory, inappropriate or rude about individuals.

Staff Responsibilities

Senior Management Team

To guide the school's priorities and policy decisions, including ensuring all School functions comply with relevant legislation, such as the UK GDPR and the DPA 2018.

Senior Information Risk Owner

To guide and where appropriate, make decisions with regards to the school's compliance with the UK GDPR and the DPA 2018.

Data Protection Officer

To oversee the school's compliance efforts with the UK GDPR and the DPA 2018. To train and provide advice to the school's staff with regards to data protection. To monitor, audit and document all data protection measures taken within the school.

All Staff

To understand the contents of this policy and to ensure they understand their own responsibilities when handling personal data. To take care and minimise mistakes made such as disclosing personal information about staff and/or students to a third-party who has no right to access the information. To understand what constitutes a data breach and how to report one.

4. Disclosing personal data

4.1 Personal data must only be shared when the staff member receiving the information is satisfied there is a clear and legal basis for sharing the information.

School staff must ask appropriate questions to ensure the requester (whether internal staff or an external partner) has the appropriate legal reason to see the information they are requesting.

Where necessary, staff members are encouraged to speak to their line manager to ask advice, or contact the school Data Protection Officer

4.2 When school staff disclose personal data to another organisation, they must keep a record of what they have shared and why.

This should include;

- A description of the information given.
- The name of the person and organisation the information was given to.
- The date of disclosure.
- The reason for the information being disclosed.
- The lawful basis.

4.3 Where appropriate the school will ensure that a Data Sharing Agreement (DSA) is in place with other organisations acting as Data Controllers. This will provide a framework for the sharing of personal data.

4.4 Where school staff respond to a request for information from another organisation, they must ensure they only share relevant and accurate information.

4.5 When personal data is given internally or externally, it must be shared using a secure method.

- Egress can securely deliver emails to any email address, including Hotmail or Google Mail accounts.
- The school may have secure TLS connections with many organisations. A full list is available on BERTHA here.

5. Accuracy and relevance

5.1 It is the responsibility of the staff who receive personal information to make sure so far as possible, that it is accurate and up to date. Personal information should be checked at regular intervals, to make sure that it is still accurate. If the information is found to be inaccurate, steps must be taken to correct it. Individuals who input or update information must also make sure that it is adequate, relevant, clear and professionally worded.

6. Retention and disposal of information

6.1 The School holds a large amount of information. The UK GDPR and the DPA 2018 requires that we do not keep personal data for any longer than is necessary. Personal data should be checked at regular intervals and deleted or destroyed when it is no longer needed, provided there is no legal or other reason for holding it.

6.2 The school Records Retention and Disposal Schedule must be checked before records are disposed of, to make sure that the retention period for the information in question, has been served.

6.3 For specific information regarding retention and disposal of personal data, consult the school's Records Management policy/Retention Schedule or contact Maria Graham School Business Manager/ School's Data Protection Officer.

7. Rights of the Data Subject

7.1 Individuals have a number of rights under the UK GDPR/DPA 2018 and they are able to enact them against any organisation at time they choose.

The Rights include: -

- **The Right of Subject Access** – the right to request a copy of data held about them by an organisation and find out how it is used.
- **The Right of Rectification** – the right to ask for inaccurate or incorrect information to be corrected or removed.
- **The Right of Data Portability** – the right to move data from one organisation to another. This could apply when moving bank accounts or energy suppliers.
- **The Right to Be Forgotten (Erasure)** – the right to ask for data to be removed by the organisation that holds it.
- **The Right of Restriction** – the right to stop information being used whilst a complaint is made.
- **The Right of Objection** – the right to ask an organisation to stop using their data. This is particularly used with regards to direct marketing.

7.2 The school has one calendar month (30 days) to respond to an individual's request to enact their Rights. This is provided the applicant has put their request in writing and suitable identification has been supplied.

7.3 If an individual wants to make an information rights request, such as a Subject Access Request, they should complete the school's Information Rights Request Form, which can be accessed via Maria Graham, School Business Manager/ Data Protection Officer.

7.4 A request must be made to the school Headteacher and the school's Data Protection Officer can provide oversight with regard to the handling of the request.

7.5 Requests will be considered in line with the individual's legal rights and the school's legal obligations.

7.6 Where an information rights request is made electronically any information provided will be in a commonly used electronic format.

7.7 Any information supplied will be free of charge. However, the school may impose a fee to comply with requests for further copies of the same information.

7.8 Where a request is unfounded, excessive, or repetitive, a fee may be charged by the school.

7.9 A fee will be based on the administrative cost of providing the information.

7.10 Those with parental authority are able to make a request to access a child's education record under education regulations, this is separate from the individual rights requests that are available under the UK GDPR. These requests must be made in writing to Maria Graham, School Business Manager/ Data Protection Officer, the school will provide the information within 15 school days. The school can, if it chooses, make a charge for these requests, however, they will not exceed the cost of supply.

8. Reporting security incidents/data breaches

8.1 As a Data Controller (organisation that determines the purpose of processing personal data) the school has a responsibility to monitor and investigate all incidents that occur within the organisation that involve any of the UK GDPR/DPA 2018 principles being breached.

All incidents need to be identified immediately, reported using the School Data Breach Report Form which is available via the school office. All incidents will be investigated by the school Data Protection Officer

Where an incident occurs, staff must inform the Data Protection Officer as soon as possible. The school has a responsibility to report all serious incidents to the Information Commissioner's Office within 72 hours of discovery. This will be done by the school Data Protection Officer.

Staff are advised to contain all incidents as quickly as possible, either by retrieving information sent in error, restricting access to personal data, or asking accidental recipients of school data to confirm personal data incorrectly shared has been deleted.
All relevant incidents and risks that are identified should be reported regardless of how trivial they may seem. The school must constantly evaluate and improve its data protection and information security practices to address the new risks it uncovers. This is to stop breaches from occurring or reoccurring as the case may be.

8.2 Specific procedures have been developed for the reporting of all information security incidents and weaknesses. It is designed to make sure that all relevant information is communicated correctly so that timely corrective action can be taken.

- Guidance for employees on Information Security including reporting an incident; and
- Actions for senior managers in reporting an information security incident.

8.3 All employees (permanent, temporary and external users), Governors and volunteers must be aware of the procedures and obligations in place for reporting the different types of incidents and weaknesses which may have an impact on the security of the school's information assets.

9 Data Protection by Design

9.1 The school will meet the requirements of the UK GDPR and the DPA 2018 by building data protection into all new projects from the start and employing appropriate technical and organisational measures to keep personal data secure. This will be achieved through completing Data Protection Impact Assessments (DPIAs)

9.2 A DPIA is a process of assessing the risks to privacy and to personal data in a project. A DPIA enables the school to identify risks and problems at an early stage in the project, meaning that changes can be made quickly and without incurring expenses.

9.3 A DPIA will be carried out when using new technologies or when processing is likely to result in high risk to the rights and freedoms of individuals.

9.4. A DPIA will be used for more than one project where necessary.

9.5 High risk processing includes, but is not limited to, the following:

- Systematic and extensive profiling activities, such as profiling.
- Large scale processing of special categories of personal data which is in relation to criminal convictions or offences.
- The use of CCTV.
- The use of EdTech applications e.g. TimesTables Rockstars, PurpleMash etc. That involve of processing of pupil level personal data.

9.6 The school has a DPIA template that will be used to ensure all required information is included and considered correctly.

9.7 Where a DPIA indicates high risk data processing, the matter will be referred to the Data Protection Officer who may consult the ICO in order to seek its opinion as to whether the processing operation complies with data protection laws.

9.8 Information within the DPIA will assist the completion of the school' Record of Processing.

9.9 Contact the school Data Protection Officer for further information regarding DPIAs.

The school's Data Protection Officer is available for advice and guidance regarding all aspects of data protection and UK GDPR. Please contact: -

Data Protection Officer Maria Graham, School Business Manager/ Data Protection Officer

Email: maria.graham@knowsley.gov.uk