St. Michael's Church School

Data Protection Policy

Policy Review Schedule

Version	Author	Summary	Review Date	Next Date
1.0	P Nuzzo	New Policy	July 2017	July 2019
1.1	P Nuzzo	Updated	July 2019	July 2021

Contents

1. Introduction

St. Michael's Church School collects and uses personal information about staff, students, parents or carers and other individuals who come into contact with the school. This information is gathered in order to enable us to provide educational and other associated services. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

In collecting, processing, sharing and disposing of personal information relating to living individuals, St. Michael's Church School is bound by the Data Protection Act (DPA) 2018 and associated General Data Protection Regulation (GDPR).

The Information Commissioner's Office enforces the Regulation, issues relevant guidance and registers personal data sets held by any organisation.

Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

St. Michael's Church School uses CCTV.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition
Personal data **GDPR Article 4 (1)** 'personal data' means any information relating to an identified or identifiable	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials)

natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one of more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of that natural person;	• Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data **GDPR Article 9 (1)** 'processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited; **GDPR Article 9 (1)** shall not apply if GDPR Article 9 (2)(c)processing is necessary to protect the vial interests of the data subect or of another natural person where the data subject is not physically or legally incapable of giving consent. 9(2)(g) processing is necessary for reasons of substantial public interest	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing **GDPR Article 4 (2)**	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Data subject **Child / Parent / Empolyee**	The identified or identifiable individual whose personal data is held or processed.
Data controller **GDPR Article 4 (7)** **ST MICHAEL'S CHURCH SCHOOL is the Data Controller**	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor **GDPR Article 4 (8)** **Employees and Appropriate Third party are 'Data Processors at ST MICHAEL'S CHURCH SCHOOL**	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach **GDPR Article 4 (12)**	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The Data Controller

As a Data Controller, St. Michael's Church School must register itself with the Information Commissioners Office (ICO) annually. This document sets out the school's policy for compliance with the General Data Protection Regulation (GDPR).

5. Roles and responsibilities

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

Governing board

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

Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

- Must be in a position to undertake their tasks independently – report to Head Teacher directly
- Be point of contact for staff and parents for data protection issues
- Support with Privacy Notices
- Review and provide assistance for any respective policies
- Overview of Data Protection processes carried out in a school
- Offer regular advice to school personnel and regular updates
- Be involved in timely manner in all data protection issues
- Inform and advise the school, processors and employees of obligations
- Monitor data protection compliance
- Advise as required on Data Protection Impact Assessments (DPIA's)
- To co-operate with supervisory authority, Information Commissioner's Authority (ICO)
- To act as contact point for the supervisory authority (ICO)
- Have due regard to the risk associated with processing, taking account of nature, scope and context of processing.
- St. Michael's Church School employs The ICT Service as their DPO; our designated consultant is Mrs Donna Flynn she can be contacted at dpo@theictservice.org.uk

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Our DPO is The ICT Service and our designated consultant is Mrs Donna Flynn; she can be contacted at dpo@theictservice.org.uk

Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis.

All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the Headteacher or DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed

- If they are unsure whether or not they have a lawful basis to use personal data in a particular way
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

All staff have a responsibility to abide by the principles of the Data Protection Act. Any breach of this policy could lead to disciplinary action being taken.

School Business Manager

- Maintaining the notification of registration for St. Michael's Church School with the Information Commissioner's Office on an annual basis

Head Teacher & School Business Manager

- Providing guidance to ensure all staff are aware of their data protection responsibilities under the act
- Responsible for managing and reporting data breaches to the schools Data Protection Officer
- Providing guidance to process Subject Access Requests and Freedom of Information requests
- Ensuring appropriate and adequate training is available to staff
- Ensuring staff are compliant with this policy and any associated procedures

6. Data protection principles

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the General Data Protection Regulation 2018, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.
All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

What is Personal Information?

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held.

The Six Guiding Principles

The General Data Protection Regulation 2018 establishes six enforceable principles and St. Michael's Church School as a registered Data Controller under the Act, will comply with these principles below:

- Personal data shall be processed lawfully, fairly and transparently in relation to the data subject (whereby the data subject is a child under 13 years of age).
- Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date; 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.
- 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 is processed.
- Personal data shall be processed in a manner that 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.

The Act creates a single framework for access to personal information about living individuals held in both paper and electronic form.

See St. Michael's Church School guidance on what to do when a Subject Access Request (SAR) is received (page 13).

7. Collecting personal data

Data Held by St. Michael's Church School with respect to School Personnel and Contacts of the school (people with parental responsibility) should include the following

Personal and Special Categories data [GDPR Articles 9(1)] is any information – held manually or electronically – which relates directly to a living individual.

Personal Data (for those with parental responsibility)

This can include but is not limited to:

- Name and Address
- Contact Number
- E-mail address
- Date of Birth

Special Categories of Data (Pertinent to Contacts and employees) Article 9(1); which is NOT processed without specific authorisation includes the following headings:

- Race or ethnic origin
- Political opinion/s
- Religious or other beliefs
- Trade union membership
- Physical or mental health or condition
- Sexual orientation
- Genetic and Biometric data
- The commission or alleged commission of offences, court sentences or allegations under investigation

The following (not an exhaustive list) should be given consideration for employees whilst processing to comply with Special Categories of personal data included in GDPR Article 9(2)(a)(b)(c)(i)

- Qualifications
- Income level
- Employment history
- Bank Details

Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

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

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

GDPR Article9 (2) (c) processing is necessary to protect the vital interest of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

Limitation, minimisation and accuracy

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

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymized. This will be done in accordance with the school's record retention schedule/records management policy.

8. Processing personal data

Employees of St. Michael's Church School, when working with personal data, will adhere to the following:

- Only collect data necessary to carry out the purpose that the task relates to.
- Respond to requests for access to personal data within one calendar month.
- Treat all personal information with equal respect for confidentiality and security whether in written, spoken or electronic form.
- Share personal or sensitive data with informed consent. Where appropriate, the school may share information without consent if, in the school's judgement, there is a good reason to do so, such as the safety and well-being of the child/children involve and others who may affected.
- Only use third parties to collect and process school's data where appropriate sharing agreements are in place, ensuring the protection of the data.
- Only retain personal data for a specified time period defined by the Schools Retention Schedule.
- Not delay data sharing where it is necessary to protect the vital interests of any individual.
- Seek approval from senior management before disclosing information for research purposes.

9. Sharing personal data

St. Michael's Church School understands that it is most important that people remain confident that their personal information is kept safe and secure, and that the school maintain the privacy of the individual, whilst sharing information to deliver better services. It is therefore important that the school can share information appropriately as part of their day-to-day practice while protecting data when sharing.

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

St. Michael's Church School will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

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

St. Michael's Church School may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

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

10. Information sharing

St. Michael's Church School understands that it is most important that people remain confident that their personal information is kept safe and secure, and that the school maintain the privacy of the individual, whilst sharing information to deliver better services. It is therefore important that the school can share information appropriately as part of their day-to-day practice while protecting data when sharing.

Third Party organisations must follow the specific Information Sharing Agreements (ISAs) set out by St. Michael's Church School when sharing data. ISAs provide a framework for the secure and confidential obtaining, holding, recording, storing and sharing of information between the school and third parties: All associated third parties will have agreements linked up to the school's Information Asset Register (IAR) that is completed with involvement from ALL School personnel.

Robust IT security systems and measures must be in place to protect the school's electronic data and its IT infrastructure from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.

11. Subject Access Requests and other rights of individuals

Subject access requests

Individuals have a right to make a 'subject access request' (SAR) 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 purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:

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

If staff receive a subject access request they must immediately forward it to the DPO.

Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 13 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

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

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

Other data protection rights of the individual

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

- Withdraw their consent to processing at any time

- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

12. **Freedom of Information Requests (FOIs)**

The Freedom of Information Act 2000 (FOIA) provides public access to information held by schools. It does this in two ways: schools are obliged to publish certain information about their activities and members of the public are entitled to request information from schools.

St. Michael's Church School will comply with Freedom of Information requests and release non-personal and non-confidential information held by the school, after applying any relevant exemptions to protect certain categories of data.

The Act requires that all requests must be in writing (to include letters, faxes and e-mails). Requests must state clearly what information is required and must provide the name of the person with an address for correspondence.

On receipt of a FOI request, a school must respond promptly and in any event within 20 working days.

For communicating a FOI request in the first instance you will need to email: https://www.cambridgeshire.gov.uk/freedom-of-information-request/ See also Freedom of Information Policy.

13. Parental requests to see the educational record

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

Appeals & Role of the ICO

In the event of a complaint or challenge regarding an information request response, whether this is a SAR or an FOI, the initial request, decision audit trail, correspondence and information released will be reviewed.

If the requestor is dissatisfied with the appeal outcome they may seek an independent review by the Information Commissioner.

The Information Commissioner is an **independent official appointed by the Crown** to oversee the General Data Protection Regulation and has the authority to demand disclosure.

In the first instance however, the Information Commissioner will usually expect that individuals will have taken the matter up first with the School.

St. Michael's Church School will comply with all notices and guidance issued by the Information Commissioner.

14. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to Mr M Cruddace Site Manager

Photographs and videos

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

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.

- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

15. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

Data security and storage of records

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

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment see our acceptable use policy.

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

Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

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

Personal data breaches

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

In the unlikely event of a suspected data breach, we will follow the procedure as set out on page 20.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymized dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

Training

All staff and governors are provided with data protection training as part of their induction process, as well as receiving regular support from our designated DPO.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

Monitoring arrangements

Our DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the full governing board.

Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Online Safety Policy
- Acceptable use of ICT
- Safeguarding

16. Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the Headteacher and the Chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

    If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision, in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school computer system. Where the ICO must be notified, the DPO will do

this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

  - A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts and cause
  - Effects
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored on the school's computer system.
- The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted
- Details of pupil premium interventions for named children being published on the school website
- Non-anonymised pupil exam results or staff pay information being shared with governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked and parents' financial details stolen

Dealing with breaches of the GDPR

St. Michael's Church School holds personal and sensitive data relating to employees, children and their families.

Every care must be taken to protect personal data and to avoid a data protection breach. In the unlikely event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible.

What is a data breach?

Inadvertent breaches of confidentiality can occur. The following are examples and not limited to:

- Reading confidential files when there is no requirement to do so
- Giving excessive information out when less would suffice
- Sending information in error eg.to a wrong email address
- Files/records removed from the office and lost
- Unencrypted devices used and lost containing personal/sensitive details
- Information that hasn't been redacted correctly before publishing

Known breaches in confidentiality must be reported to the school's Headteacher or someone in the Leadership immediately so it can be recorded, and a formal investigation carried out.

What to do when a breach occurs:

There are four elements in dealing with a data breach. These are:

1. Containment and recovery
2. Assessment of ongoing risk
3. Notification of breach
4. Evaluation and response

See the schools Data Breach Process for more information in the event of a data breach.

Remember you must report these IMMEDIATELY as there are only 72 hours to report an instance from it being assessed to it being reported to The ICO, please ensure you give your DPO adequate time!

Training

St. Michael's Church School will arrange training for all staff, so they are fully aware of their obligations and responsibilities under the Data Protection Act 2018 and associated GDPR Legislation.

Confidentiality

St. Michael's Church School must ensure that all personal data is treated confidentially. All staff must comply with the Schools Data Protection Policy, Information Security Policy, Records Management Policy, Subject Access Request Process, Freedom of Information Request Process and Data Breach Process.

What happens if this policy is breached?

Failure to adhere to this or any related policy, could lead to disciplinary action.

Policy Authorisation

Name/Role	**Date**	**Version**
Designated School's Data Protection Lead **Mrs P Nuzzo**	July 2019	1.1
Head Teacher **Mrs R Smith**	July 2019	1.1
Chair of Governors **Mrs A Kupara**	July 2019	1.1
Designated DPO **Mrs S Hibbitt**	July 2019	1.1