**Data Protection Policy**

**Name of School:** St Mary’s CofE Primary School

**Date of Policy:** September 2019

**Member of Staff Responsible:** Governing Body Policy

**Review Date:** May 2021

**Consultation:** This policy has been drawn up by the staff and governors at St Mary’s School, following recommendations from Birmingham Local Authority, the Department for Education, Judicium Education - the school’s Data Protection Officer (DPO) and the Information Commissioner’s Office (ICO).

**ETHOS STATEMENT**

In accordance with the aims of the school, the Governing Body of St Mary’s believe that all members of the school community should be esteemed, cared for, treated courteously and encouraged to make their unique contribution. Within our Christian ethos of love, forgiveness and justice for each person as a valued child of God, we aim to develop understanding and respect for each other’s faith, culture.

We also uphold Article 29 from the UN Convention of Rights of the Child ‘Education must develop every child's personality, talents and abilities to the full. It must encourage the child's respect for human rights, as well as respect for their parents, their own and other cultures and the environment.’

**Introduction**

The General Data Protection Regulation (GDPR) ensures a balance between an individual’s rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The School will protect and maintain a balance between data protection rights in accordance with the GDPR. This policy sets out how we handle the personal data of our pupils, parents, suppliers, employees, workers and other third parties.

This policy does not form part of any individual’s terms and conditions of employment with the School and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the School’s Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

**SECTION 1 - DEFINITIONS**

**Personal data**

Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

Personal data can be factual (for examples a name, email address, location or date of birth) or an opinion about that person’s actions or behaviour.

Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

**Special Category Data**

Previously termed “Sensitive Personal Data”, Special Category Data is similar by definition and refers to data concerning an individual Data Subject’s racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions.

**Data Subject**

An individual about whom such information is stored is known as the Data Subject. It includes but is not limited to employees.

**Data Controller**

The organisation storing and controlling such information (i.e. the school) is referred to as the Data Controller.

**Processing**

Processing data involves any activity that involves the use of personal data. This includes but is not limited to: obtaining, recording or holding data or carrying out any operation or set of operations on that data such as organisation, amending, retrieving using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

**Data Protection Impact Assessment (DPIA)**

DPIAs are a tool used to identify risks in data processing activities with a view to reducing them.

**Criminal Records Information**

This refers to personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.

**SECTION 2 - WHEN CAN THE SCHOOL PROCESS PERSONAL DATA**

**Data Protection Principles**

The School are responsible for and adhere to the principles relating to the processing of personal data as set out in the GDPR.

The principles the School must adhere to are set out below.

**Principle 1: Personal data must be processed lawfully, fairly and in a transparent manner**

The School only collect, process and share personal data fairly and lawfully and for specified purposes. The School must have a specified purpose for processing personal data and special category of data as set out in the GDPR.

Before the processing starts for the first time we will review the purposes of the particular processing activity and select the most appropriate lawful basis for that processing. We will then regularly review those purposes whilst processing continues in order to satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose).

Personal Data

The School may only process a data subject’s personal data if one of the following fair processing conditions are met: -

* The data subject has given their consent;
* The processing is necessary for the performance of a contract with the data subject or for taking steps at their request to enter into a contract;
* To protect the data subject’s vital interests;
* To meet our legal compliance obligations (other than a contractual obligation);
* To perform a task in the public interest or in order to carry out official functions as authorised by law;
* For the purposes of the School’s legitimate interests where authorised in accordance with data protection legislation. This is provided that it would not prejudice the rights and freedoms or legitimate interests of the data subject.

Special Category Data

The School may only process special category data if they are entitled to process personal data (using one of the fair processing conditions above) AND one of the following conditions are met: -

* The data subject has given their explicit consent;
* The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed on the School in the field of employment law, social security law or social protection law. This may include, but is not limited to, dealing with sickness absence, dealing with disability and making adjustments for the same, arranging private health care insurance and providing contractual sick pay;
* To protect the data subject’s vital interests;
* To meet our legal compliance obligations (other than a contractual obligation);
* Where the data has been made public by the data subject;
* To perform a task in the substantial public interest or in order to carry out official functions as authorised by law;
* Where it 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;
* Where it is necessary for reasons of public interest in the area of public health;
* The processing in necessary for archiving, statistical or research purposes.

The School identifies and documents the legal grounds being relied upon for each processing activity.

Consent

Where the School relies on consent as a fair condition for processing (as set out above), it will adhere to the requirements set out in the GDPR.

Consent must be freely given, specific, informed and be an unambiguous indication of the data subject’s wishes by which they signify agreement to the processing of personal data relating to them. Explicit consent requires a very clear and specific statement to be relied upon (i.e. more than just mere action is required).

A data subject will have consented to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity will not amount to valid consent.

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured.

If explicit consent is required, the School will normally seek another legal basis to process that data. However, if explicit consent is required the data subject will be provided with full information in order to provide explicit consent.

The School will keep records of consents obtained in order to demonstrate compliance with consent requirements under the GDPR.

**Principle 2: Personal data must be collected only for specified, explicit and legitimate purposes**

Personal data will not be processed in any matter that is incompatible with the legitimate purposes.

The School will not use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the data subject of the new purpose (and they have consented where necessary).

**Principle 3: Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed**

The School will only process personal data when our obligations and duties require us to. We will not collect excessive data and ensure any personal data collected is adequate and relevant for the intended purposes.

When personal data is no longer needed for specified purposes, the School shall delete or anonymise the data.

**Principle 4: Personal data must be accurate and, where necessary, kept up to date**

The School will endeavour to correct or delete any inaccurate data being processed by checking the accuracy of the personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out of date personal data.

Data subjects also have an obligation to ensure that their data is accurate, complete, up to date and relevant. Data subjects have the right to request rectification to incomplete or inaccurate data held by the School.

**Principle 5: Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed**

Legitimate purposes for which the data is being processed may include satisfying legal, accounting or reporting requirements. The School will ensure that they adhere to legal timeframes for retaining data.

We will take reasonable steps to destroy or erase from our systems all personal data that we no longer require. We will also ensure that data subjects are informed of the period for which data is stored and how that period is determined in our privacy notices.

Please refer to the School’s Retention Policy for further details about how the School retains and removes data.

**Principle 6: Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage**

In order to assure the protection of all data being processed, the School will develop, implement and maintain reasonable safeguard and security measures. This includes using measures such as: -

* Encryption;
* Pseudonymisation (this is where the School replaces information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure);
* Ensuring authorised access (i.e. that only people who have a need to know the personal data are authorised to access it);
* Adhering to confidentiality principles;
* Ensuring personal data is accurate and suitable for the process for which it is processed.

The School follow procedures and technologies to ensure security and will regularly evaluate and test the effectiveness of those safeguards to ensure security in processing personal data.

The School will only transfer personal data to third party service providers who agree to comply with the required policies and procedures and agree to put adequate measures in place.

**Sharing Personal Data**

The School will generally not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. These include if the third party: -

* Has a need to know the information for the purposes of providing the contracted services;
* Sharing the personal data complies with the privacy notice that has been provided to the data subject and, if required, the data subject’s consent has been obtained;
* The third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
* The transfer complies with any applicable cross border transfer restrictions; and
* A fully executed written contract that contains GDPR approved third party clauses has been obtained.

There may be circumstances where the School is required either by law or in the best interests of our pupils, parents or staff to pass information onto external authorities, for example, the local authority, Ofsted or the department of health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

The intention to share data relating to individuals to an organisation outside of our School shall be clearly defined within written notifications and details and basis for sharing that data given.

**Transfer of Data Outside the European Economic Area (EEA)**

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined.

The School will not transfer data to another country outside of the EEA without appropriate safeguards being in place and in compliance with the GDPR. All staff must comply with the School’s guidelines on transferring data outside of the EEA. For the avoidance of doubt, a transfer of data to another country can occur when you transmit, send, view or access that data in that particular country.

**SECTION 3 - DATA SUBJECT’S RIGHTS AND REQUESTS**

Personal data must be made available to data subjects as set out within this policy and data subjects must be allowed to exercise certain rights in relation to their personal data.

The rights data subjects have in relation to how the School handle their personal data are set out below: -

* + 1. (Where consent is relied upon as a condition of processing) To withdraw consent to processing at any time;
    2. Receive certain information about the School’s processing activities;
    3. Request access to their personal data that we hold (see “Subject Access Requests” at Appendix 1);
    4. Prevent our use of their personal data for marketing purposes;
    5. Ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;
    6. Restrict processing in specific circumstances;
    7. Challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
    8. Request a copy of an agreement under which personal data is transferred outside of the EEA;
    9. Object to decisions based solely on automated processing;
    10. Prevent processing that is likely to cause damage or distress to the data subject or anyone else;
    11. Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
    12. Make a complaint to the supervisory authority; and
    13. In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

If any request is made to exercise the rights above, it is a requirement for the relevant staff member within the School to verify the identity of the individual making the request.

**Direct Marketing**

The School are subject to certain rules and privacy laws when marketing. For example, a data subject’s prior consent will be required for electronic direct marketing (for example, by email, text or automated calls).

The School will explicitly offer individuals the opportunity to object to direct marketing and will do so in an intelligible format which is clear for the individual to understand. The School will promptly respond to any individual objection to direct marketing.

**Employee Obligations**

Employees may have access to the personal data of other members of staff, suppliers, parents or pupils of the School in the course of their employment or engagement. If so, the School expects those employees to help meet the School’s data protection obligations to those individuals. Specifically, you must: -

* Only access the personal data that you have authority to access, and only for authorised purposes;
* Only allow others to access personal data if they have appropriate authorisation;
* Keep personal data secure (for example by complying with rules on access to school premises, computer access, password protection and secure file storage and destruction;
* Not to remove personal data or devices containing personal data from the School premises unless appropriate security measures are in place (such as pseudonymisation, encryption, password protection) to secure the information;
* Not to store personal information on local drives.

**SECTION 4 - ACCOUNTABILITY**

The School will ensure compliance with data protection principles by implementing appropriate technical and organisational measures. We are responsible for and demonstrate accountability with the GDPR principles.

The School have taken the following steps to ensure and document GDPR compliance: -

**Data Protection Officer (DPO)**

Please find below details of the School’s Data Protection Officer: -

Data Protection Officer: Judicium Consulting Limited

Address: 72 Cannon Street, London, EC4N 6AE

Email: [dataservices@judicium.com](mailto:dataservices@judicium.com)

Web: www.judiciumeducation.co.uk

Telephone: 0203 326 9174

Lead Contact: Craig Stilwell

The DPO is responsible for overseeing this data protection policy and developing data-related policies and guidelines.

Please contact the DPO with any questions about the operation of this Data Protection Policy or the GDPR or if you have any concerns that this policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances: -

1. If you are unsure of the lawful basis being relied on by the School to process personal data;
2. If you need to rely on consent as a fair reason for processing (please see below the section on consent for further detail);
3. If you need to draft privacy notices or fair processing notices;
4. If you are unsure about the retention periods for the personal data being processed [this would fall under the School’s data retention policy in the first instance];
5. If you are unsure about what security measures need to be put in place to protect personal data;
6. If there has been a personal data breach (this would be managed under the procedure set out in the School’s breach notification policy);
7. If you are unsure on what basis to transfer personal data outside the EEA;
8. If you need any assistance dealing with any rights invoked by a data subject;
9. Whenever you are engaging in a significant new (or a change in) processing activity which is likely to require a data protection impact assessment or if you plan to use personal data for purposes other than what it was collected for;
10. If you plan to undertake any activities involving automated processing or automated decision making;
11. If you need help complying with applicable law when carrying out direct marketing activities;
12. If you need help with any contracts or other areas in relation to sharing personal data with third parties.

**Personal Data Breaches**

The GDPR requires the School to notify any applicable personal data breach to the Information Commissioner’s Office (ICO).

We have put in place procedures to deal with any suspected personal data breach and will notify data subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person designated as the key point of contact for personal data breaches (this is the Headteacher).

**Transparency and Privacy Notices**

The School will provide detailed, specific information to data subjects. This information will be provided through the School’s privacy notices (see Appendices) which are concise, transparent, intelligible, easily accessible and in clear and plain language so that a data subject can easily understand them. Privacy notices sets out information for data subjects about how the School use their data and the School’s privacy notices are tailored to suit the data subject.

Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we will provide the data subject with all the information required by the GDPR including the identity of the data protection officer, the School’s contact details, how and why we will use, process, disclose, protect and retain personal data. This will be provided in our privacy notices. When personal data is collected indirectly (for example from a third party or publically available source), we will provide the data subject with the above information as soon as possible after receiving the data. The School will also confirm whether that third party has collected and processed data in accordance with the GDPR.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as “children” under the GDPR

**Privacy By Design**

The School adopt a privacy be design approach to data protection to ensure that we adhere to data compliance and to implement technical and organisational measures in an effective manner.

Privacy by design is an approach that promotes privacy and data protection compliance from the start. To help us achieve this, the School takes into account the nature and purposes of the processing, any cost of implementation and any risks to rights and freedoms of data subjects when implementing data processes.

**Data Protection Impact Assessments (DPIAs)**

In order to achieve a privacy by design approach, the School conduct DPIAs for any new technologies or programmes being used by the School which could affect the processing of personal data. In any event the School carries out DPIAs when required by the GDPR in the following circumstances: -

* For the use of new technologies (programs, systems or processes) or changing technologies;
* For the use of automated processing;
* For large scale processing of special category data;
* For large scale, systematic monitoring of a publicly accessible area (through the use of CCTV).

Our DPIAs contain: -

* A description of the processing, its purposes and any legitimate interests used;
* An assessment of the necessity and proportionality of the processing in relation to its purpose;
* An assessment of the risk to individuals; and
* The risk mitigation measures in place and demonstration of compliance.

**Record Keeping**

The School are required to keep full and accurate records of our data processing activities. These records include: -

* The name and contact details of the School;
* The name and contact details of the Data Protection Officer;
* Descriptions of the types of personal data used;
* Description of the data subjects;
* Details of the School’s processing activities and purposes;
* Details of any third party recipients of the personal data;
* Where personal data is stored;
* Retention periods; and
* Security measures in place.

**Training**

The School will ensure all relevant personnel have undergone adequate training to enable them to comply with data privacy laws.

**Audit**

The School through its data protection officer regularly test our data systems and processes in order to assess compliance. These are done through data audits which take place annually in order to review use of personal data.

**Related Policies**

Staff should refer to the following policies that are related to this data protection policy:

-CCTV; Data Breach; Data Retention.

These policies are also designed to protect personal data and can be obtained from the school upon request.

**Monitoring**

We will monitor the effectiveness of this and all of our policies and procedures and conduct a full review and update as appropriate.

Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the School.

**Appendix 1 – Subject Access Requests**

Under Data Protection Law, Data Subjects have a general right to find out whether the School hold or process personal data about them, to access that data, and to be given supplementary information. This is known as the right of access, or the right to make a data subject access request (SAR). The purpose of the right is to enable the individual to be aware of, and verify, the lawfulness of the processing of personal data that the School are undertaking.

A Data Subject has the right to be informed by the School of the following: -

1. Confirmation that their data is being processed;
2. Access to their personal data;
3. A description of the information that is being processed;
4. The purpose for which the information is being processed;
5. The recipients/class of recipients to whom that information is or may be disclosed;
6. Details of the School’s sources of information obtained;
7. In relation to any Personal Data processed for the purposes of evaluating matters in relation to the Data Subject that has constituted or is likely to constitute the sole basis for any decision significantly affecting him or her, to be informed of the logic of the Data Controller’s decision making. Such data may include, but is not limited to, performance at work, creditworthiness, reliability and conduct; and
8. Other supplementary information.

**How to recognise a subject access request**

A data subject access request is a request from an individual (or from someone acting with the authority of an individual, e.g. a solicitor or a parent making a request in relation to information relating to their child):

* for confirmation as to whether the School process personal data about him or her and, if so
* for access to that personal data
* and/or certain other supplementary information

A valid SAR can be both in writing (by letter, email) or verbally (e.g. during a telephone conversation). The request may refer to the GDPR and/or to ‘data protection’ and/or to ‘personal data’ but does not need to do so in order to be a valid request. For example, a letter which states ‘please provide me with a copy of information that the School hold about me’ will be a data subject access request and should be treated as such.

A data subject is generally only entitled to access their own personal data, and not information relating to other people.

**How to make a data subject access request**

Whilst there is no requirement to do so, we encourage any individuals who wish to make such a request to make the request in writing, detailing exactly the personal data being requested. This allows the School to easily recognise that you wish to make a data subject access request and the nature of your request. If the request is unclear/ vague we may be required to clarify the scope of the request which may in turn delay the start of the time period for dealing with the request.

**What to do when you receive a data subject access request**

All data subject access requests should be immediately directed to the Headteacher who should contact Judicium as DPO in order to assist with the request and what is required.

**Acknowledging the request**

When receiving a SAR the School shall acknowledge the request as soon as possible and inform the requester about the statutory deadline (of one calendar month) to respond to the request.

In addition to acknowledging the request, the School may ask for:

* proof of ID (if needed);
* further clarification about the requested information;
* if it is not clear where the information shall be sent, the School must clarify what address/email address to use when sending the requested information; and/or
* consent (if requesting third party data).

The School should work with their DPO in order to create the acknowledgment.

**Verifying the identity of a requester or requesting clarification of the request**

Before responding to a SAR, the School will take reasonable steps to verify the identity of the person making the request. In the case of current employees, this will usually be straightforward. The School is entitled to request additional information from a requester in order to verify whether the requester is in fact who they say they are. Where the School has reasonable doubts as to the identity of the individual making the request, evidence of identity may be established by production of a passport, driving license, a recent utility bill with current address, birth/marriage certificate, credit card or a mortgage statement.

If an individual is requesting a large amount of data the School may ask the requester for more information for the purpose of clarifying the request, but the requester shall never be asked why the request has been made. The School shall let the requestor know as soon as possible where more information is needed before responding to the request.

In both cases, the period of responding begins when the additional information has been received. If the School do not receive this information, they will be unable to comply with the request.

**Requests made by third parties or on behalf of children**

The school need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party’s responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney. The School may also require proof of identity in certain circumstances.

When requests are made on behalf of children, it is important to note that even if a child is too young to understand the implications of subject access rights, it is still the right of the child, rather than of anyone else such as a parent or guardian, to have access to the child’s personal data. Before responding to a SAR for information held about a child, the School should consider whether the child is mature enough to understand their rights. If the school is confident that the child can understand their rights, then the School should usually respond directly to the child or seek their consent before releasing their information.

It shall be assessed if the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, it should be taken into account, among other things:

• the child’s level of maturity and their ability to make decisions like this;

• the nature of the personal data;

• any court orders relating to parental access or responsibility that may apply;

• any duty of confidence owed to the child or young person;

• any consequences of allowing those with parental responsibility access to the child’s or young person’s information. This is particularly important if there have been allegations of abuse or ill treatment;

• any detriment to the child or young person if individuals with parental responsibility cannot access this information; and

• any views the child or young person has on whether their parents should have access to information about them.

Generally, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. In relation to a child 12 years of age or older, then provided that the School is confident that they understand their rights, and there is no reason to believe that the child does not have the capacity to make a request on their own behalf, the School will require the written authorisation of the child before responding to the requester, or provide the personal data directly to the child.

The School may also refuse to provide information to parents if there are consequences of allowing access to the child’s information – for example if it is likely to cause detriment to the child.

**Fee for responding to a SAR**

The School will usually deal with a SAR free of charge. Where a request is considered to be manifestly unfounded or excessive a fee to cover administrative costs may be requested.

**Time Period for Responding to a SAR**

The School has one calendar month to respond to a SAR. This will run from the day that the request was received or from the day when any additional identification or other information requested is received, or payment of any required fee has been received.

The period for response may be extended by a further two calendar months in relation to complex requests. What constitutes a complex request will depend on the particular nature of the request. The DPO must always be consulted in determining whether a request is sufficiently complex as to extend the response period.

Where a request is considered to be sufficiently complex as to require an extension of the period for response, the School will need to notify the requester within one calendar month of receiving the request, together with reasons as to why this extension is considered necessary.

**School closure periods**

Requests received during or just before school closure periods may not be able to be responded to within the one calendar month response period. This is because the school will be closed during this period. As a result, it is unlikely that your request will be able to be dealt with during this time.

We may not be able to acknowledge your request during this time (i.e. until a time when we receive the request), however, if we can acknowledge the request we may still not be able to deal with it until the school re-opens. The School will endeavour to comply with requests as soon as possible and will keep in communication with you as far as possible. If your request is urgent, please provide your request during term times and not during/close to closure periods.

**Information to be provided in response to a request**

The individual is entitled to receive access to the personal data we process about him or her.

The information should be provided in a way that is concise, transparent, easy to understand and easy to access using clear and plain language, with any technical terms, abbreviations or codes explained. The response shall be given in writing if the SAR was made in writing in a commonly-used electronic format.

The information that the School are required to supply in response to a SAR must be supplied by reference to the data in question at the time the request was received. However, as the School have one month in which to respond the School is allowed to take into account any amendment or deletion made to the personal data between the time the request is received and the time the personal data is supplied if such amendment or deletion would have been made regardless of the receipt of the SAR.

The School is therefore, allowed to carry out regular housekeeping activities even if this means deleting or amending personal data after the receipt of a SAR. The School is not allowed to amend or delete data to avoid supplying the data.

**How to locate information**

The personal data the School need to provide in response to a data subject access request may be located in several of the electronic and manual filing systems. This is why it is important to identify at the outset the type of information requested so that the search can be focused.

**Protection of third parties -exemptions to the right of subject access**

There are circumstances where information can be withheld pursuant to a SAR. These specific exemptions and requests should be considered on a case by case basis.

The School will consider whether it is possible to redact information so that this does not identify those third parties. If their data cannot be redacted (for example, after redaction it is still obvious who the data relates to) then the School do not have to disclose personal data to the extent that doing so would involve disclosing information relating to another individual (including information identifying the other individual as the source of information) who can be identified from the information unless:

• the other individual has consented to the disclosure; or

• it is reasonable to comply with the request without that individual’s consent.

In determining whether it is reasonable to disclose the information without the individual’s consent, all of the relevant circumstances will be taken into account, including:

• the type of information that they would disclose;

• any duty of confidentiality they owe to the other individual;

• any steps taken to seek consent from the other individual;

• whether the other individual is capable of giving consent; and

• any express refusal of consent by the other individual.

It needs to be decided whether it is appropriate to disclose the information in each case. This decision will involve balancing the data subject’s right of access against the other individual’s rights. If the other person consents to the school disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, the school must decide whether to disclose the information anyway. If there are any concerns in this regard, then the DPO should be consulted.

**Other exemptions to the right of subject access**

In certain circumstances the school may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

Crime detection and prevention: The school do not have to disclose any personal data being processed for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty.

Confidential references: The School do not have to disclose any confidential references given to third parties for the purpose of actual or prospective:

* education, training or employment of the individual;
* appointment of the individual to any office; or
* provision by the individual of any service

This exemption does not apply to confidential references that the School receive from third parties. However, in this situation, granting access to the reference may disclose the personal data of another individual (i.e. the person giving the reference), which means that the School must consider the rules regarding disclosure of third-party data set out above before disclosing the reference.

Legal professional privilege: The School do not have to disclose any personal data which are subject to legal professional privilege.

Management forecasting: The School do not have to disclose any personal data processed for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity.

Negotiations: The School do not have to disclose any personal data consisting of records of intentions in relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations.

**Appendix 1 – Privacy Impact Statement (PIA) Screening Questions**

Apply these questions at the proposal stage of a project where a change to the data collected about an individual.

An answer of ‘Yes’ to any of these indicates that a PIA should be carried out. Guidance and procedures on carrying out a PIA can be found at:

<https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>

-Will the project involve the collection of new information about individuals?

-Will the project compel individuals to provide information about themselves?

-Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?

-Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?

-Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.

-Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?

-Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.

-Will the project require you to contact individuals in ways which they may find intrusive?

**Appendix 2 – Privacy Notice (Pupils)**

**St Mary’s Church of England Primary School**

**Privacy Notice (Pupils)**

**Why do we collect and use pupil information?**

We collect and use pupil information under the EU GDPR (May 2018) and specifically Article 6 where it states:

6(1)(a) – Consent of the data subject

6(1)(c) – Processing is necessary for compliance with a legal obligation

6(1)(e) – Processing is necessary for the effective discharge of a public task

**We use pupil data to:**

* support pupil learning
* monitor and report on pupils’ academic progress and their personal development
* provide appropriate pastoral care
* assess the quality of our services
* comply with the law regarding data sharing

**The categories of pupil information that we collect, hold and share include:**

* Personal information (such as name, unique pupil number and address)
* Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
* Attendance information (such as sessions attended, number of absences and absence reasons)
* Assessment information (such as progress in specific areas of the school’s curriculum)
* Relevant medical information (such as specific medical conditions and allergies)
* Special Education Needs information (such as actions in a specific support plan)
* Behavioural information (such as information relating to exclusions and racist incidents)
* Contact details of parents (name; address; telephone number; email address)

**Collecting pupil information**

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this. You will need to give active consent for this data to be processed by us. Therefore, in this school, inactivity or silence does not constitute consent.

Data related to parents (e.g. contact details) is collected and retained in order to satisfy the school’s ‘public task’ duty (i.e. in this case to be able to manage the school safely).

**Storing pupil data**

We hold pupil data for the duration of their time at the school. All data is stored securely and in accordance with clear policies and procedures for ensuring data breaches are avoided. Electronic information is held in either secure ‘cloud-based’ solutions or securely on the school’s ICT network while paper-based information is stored in secure locations.

Upon leaving the school, all data related to an individual pupil is securely transferred to their new educational setting either electronically, by personal delivery or using Royal Mail Special Delivery.

Upon leaving the school, all data related to an individual pupil’s parents is destroyed. The responsibility for establishing the legal basis for the collection and processing of this type of data transfers to the new setting.

**Who do we share pupil information with?**

We routinely share pupil information with:

* schools that the pupils attend after leaving us;
* our local authority and departments within it;
* the Department for Education (DfE);
* the NHS and specific employees (e.g. the school nurse);
* the school’s financial support service (e.g. activating access to additional funding for eligible pupils).

**Why do we share pupil information?**

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

We share pupils’ data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

The school will not share the data of pupils or family members with organisations for the purpose of marketing, advertising goods or services and direct selling.

**Data collection requirements:**

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

For more information about services for young people, please visit our local authority website ([www.birmingham.gov.uk/schools](http://www.birmingham.gov.uk/schools))

**The National Pupil Database (NPD)**

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years’ census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the pupil information we share with the department, for the purpose of data collections, go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

To find out more about the NPD, go to <https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information>.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

* conducting research or analysis
* producing statistics
* providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

* who is requesting the data
* the purpose for which it is required
* the level and sensitivity of data requested: and
* the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

-For more information about the department’s data sharing process, please visit:

<https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

-For information about which organisations the department has provided pupil information, (and for which project), please visit the following website: <https://www.gov.uk/government/publications/national-pupil-database-requests-received>

-To contact DfE: <https://www.gov.uk/contact-dfe>

**Requesting access to your personal data**

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child’s educational record, contact Ruth Price (School Office Manager) in writing. The necessary arrangements for providing this data will then be made within the timeframe specified in the school’s Data Protection Policy.

You also have the right to:

* object to processing of personal data that is likely to cause, or is causing, damage or distress
* prevent processing for the purpose of direct marketing
* object to decisions being taken by automated means
* in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
* claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner’s Office at <https://ico.org.uk/concerns/>

**Contact:**

If you would like to discuss anything in this privacy notice, please contact Mr S Smith (Headteacher). This notice should be used in conjunction with the school’s Data Protection Policy, a copy of which is available upon request.

**Appendix 3 – Privacy Notice (Employees)**

**St Mary’s Church of England Primary School**

**Privacy Notice**

**(Employees)**

**The Data Protection Act 1998: How we use your information**

We process personal data relating to those we employ to work at, or otherwise engage to work at, our school, St Mary’s CofE Primary School. This is for employment purposes to assist in the running of the school and to enable individuals to be paid. The collection of this information will benefit both national and local users by:

* improving the management of workforce data across the sector
* enabling development of a comprehensive picture of the workforce and how it is deployed
* informing the development of recruitment and retention policies
* allowing better financial modelling and planning
* enabling ethnicity and disability monitoring; and
* supporting the work of the School Teachers’ Review Body

This personal data includes identifiers such as names and National Insurance numbers and characteristics such as ethnic group, employment contracts and remuneration details, qualifications, appraisal records and absence information.

We will not share information about you with third parties without your consent unless the law allows us to. We are required, by law, to pass on some of this personal data to:

* our Local Authority (Birmingham)
* the Department for Education (DfE)

**Why do we collect and use employee information?**

We collect and use employee information under the EU GDPR (May 2018) and specifically Article 6 where it states:

6(1)(a) – Consent of the data subject

6(1)(c) – Processing is necessary for compliance with a legal obligation

6(1)(e) – Processing is necessary for the effective discharge of a public task

**Storing employee data**

We hold your data for the duration of your employment at the school. All data is stored securely and in accordance with clear policies and procedures for ensuring that data breaches are avoided. Electronic information is held in either secure ‘cloud-based’ solutions or securely on the school’s ICT network while paper-based information is stored in secure locations.

Upon leaving the school, all electronic data related to your employment is removed from the school’s electronic systems. Paper-based data is securely stored and retained by the school as archived material.

If you require more information about how we, Birmingham LA and DfE store and use your personal data please visit:

* [www.birmingham.gov.uk/schools](http://www.birmingham.gov.uk/schools)
* <https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

If you want to see a copy of information about you that we hold, please contact: Mr S Smith (Headteacher)

**Requesting access to your personal data**

Under data protection legislation, employees have the right to request access to information about them that we hold. To make a request for your personal information, contact Ruth Price (School Office Manager) in writing. The necessary arrangements for providing this data will then be made within the timeframe specified in the school’s Data Protection Policy.

You also have the right to:

* object to processing of personal data that is likely to cause, or is causing, damage or distress
* prevent processing for the purpose of direct marketing
* object to decisions being taken by automated means
* in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
* claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner’s Office at <https://ico.org.uk/concerns/>

**Contact:** If you would like to discuss anything in this privacy notice, please contact Mr S Smith (Headteacher). This notice should be used in conjunction with the school’s Data Protection Policy, a copy of which is available upon request.

**Appendix 4 – Privacy Notice (Job Applicants)**

**St Mary’s Church of England Primary School**

**Privacy Notice**

**(Job Applicants)**

St Mary’s CofE Primary School is committed to protecting the privacy and security of your personal information. This privacy notice describes how we collect and use personal information about you during and after your work relationship with us, in accordance with the General Data Protection Regulation (GDPR).

Successful candidates should refer to our privacy notice for staff for information about how their personal data is stored and collected.

**Who Collects This Information**

St Mary’s CofE Primary School is a “data controller.” This means that we are responsible for deciding how we hold and use personal information about you.

We are required under data protection legislation to notify you of the information contained in this privacy notice. This notice does not form part of any contract of employment or other contract to provide services and we may update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

**Data Protection Principles**

We will comply with the data protection principles when gathering and using personal information, as set out in our data protection policy.

**The Categories of Information That We Collect, Process, Hold and Share**

We may collect, store and use the following categories of personal information about you up to the shortlisting stage of the recruitment process: -

* Personal information and contact details such as name, title, addresses, date of birth, marital status, phone numbers and personal email addresses;
* Emergency contact information such as names, relationship, phone numbers and email addresses;
* Information collected during the recruitment process that we retain during your employment including proof of right to work in the UK, information entered on the application form, CV, qualifications;
* Details of your employment history including job titles, salary and working hours;
* Your racial or ethnic origin, sex and sexual orientation, religious or similar beliefs;
* Information regarding your criminal record as required by law to enable you to work with children;
* Details of your referees and references.

We may also collect information after the shortlisting and interview stage in order to make a final decision on where to recruit, including criminal record information, references, information regarding qualifications. We may also ask about details of any conduct, grievance or performance issues, appraisals, time and attendance from references provided by you.

**How We Collect This Information**

* We may collect this information from you, your referees, your education provider, relevant professional bodies the Home Office and from the DBS.

**How We Use Your Information**

We will only use your personal information when the law allows us to. Most commonly, we will use your information in the following circumstances: -

* Where we need to take steps to enter into a contract with you;
* Where we need to comply with a legal obligation (such as health and safety legislation, under statutory codes of practice and employment protection legislation);
* Where it is needed in the public interest or for official purposes;
* Where it is necessary for our legitimate interests (or those of a third party) and your interests, rights and freedoms do not override those interests.

Generally, the purpose of us collecting your data is to enable us to facilitate safe recruitment and determine suitability for the role. We also collect data in order to carry out equal opportunities monitoring and to ensure appropriate access arrangements are put in place if required.

If you fail to provide certain information when requested, we may not be able to take the steps to enter into a contract with you (for example if incorrect references are provided), or we may be prevented from complying with our legal obligations (such as to determine suitability to work with children).

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

**How We Use Particularly Sensitive Information**

Sensitive personal information (as defined under the GDPR as “special category data”) require higher levels of protection and further justification for collecting, storing and using this type of personal information. We may process this data in the following circumstances: -

* In limited circumstances, with your explicit written consent;
* Where we need to carry out our legal obligations in line with our data protection policy;
* Where it is needed in the public interest, such as for equal opportunities monitoring;
* Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards. Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is necessary to protect your interests (or someone else’s interests) and you are not capable of giving your consent.

**Criminal Convictions**

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where it is necessary to carry out our legal obligations. We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so.

Where appropriate we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of working for us.

**Sharing Data**

We may need to share your data with third parties, including third party service providers where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

These include the following: -

* Academic or regulatory bodies to validate qualifications/experience (for example the teaching agency);
* Referees;
* Our Local Authority in order to meet our legal obligations for sharing data with it;
* Other schools;
* DBS; and
* Recruitment and supply agencies.

We may also need to share some of the above categories of personal information with other parties, such as HR consultants and professional advisers. Usually information will be anonymised but this may not always be possible. The recipients of the information will be bound by confidentiality obligations. We may also be required to share some personal information with our regulators or as required to comply with the law.

**Retention Periods**

Except as otherwise permitted or required by applicable law or regulation, the School only retains personal data for as long as necessary to fulfil the purposes they collected it for, as required to satisfy any legal, accounting or reporting obligations, or as necessary to resolve disputes.

## How long we keep your information will depend on whether your application is successful and you become employed by us, the nature of the information concerned and the purposes for which it is processed. Full details on how long we keep personal data for is set out in our data retention policy.

**Security**

We have put in place measures to protect the security of your information (i.e. against it being accidentally lost, used or accessed in an unauthorised way). In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. Details of these measures are available in the school’s Data Protection and Data Breach policies.

Third parties will only process your personal information on our instructions and where they have agreed to treat information confidentially and to keep it secure.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

**Your Rights of Access, Correction, Erasure and Restriction**

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Under certain circumstances by law you have the right to: -

* Access your personal information (commonly known as a “subject access request”). This allows you to receive a copy of the personal information we hold about you and to check we are lawfully processing it. You will not have to pay a fee to access your personal information. However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.
* Correction of the personal information we hold about you. This enables you to have any inaccurate information we hold about you corrected.
* Erasure of your personal information. You can ask us to delete or remove personal data if there is no good reason for us continuing to process it.
* Restriction of processing your personal information. You can ask us to suspend processing personal information about you in certain circumstances, for example, if you want us to establish its accuracy before processing it.
* To object to processing in certain circumstances (for example for direct marketing purposes).
* To transfer your personal information to another party.

If you want to exercise any of the above rights, please contact the Headteacher in writing.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

**Right to Withdraw Consent**

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Headteacher. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

**How to Raise A Concern**

We hope that the school can resolve any query you raise about our use of your information in the first instance.

We have appointed a data protection officer (DPO) to oversee compliance with data protection and this privacy notice. If you have any questions about how we handle your personal information which cannot be resolve by us, then you can contact the DPO on the details below: -

Data Controller Name: Craig Stilwell

Data Controller Details: Judicium Consulting Ltd, 72 Cannon Street, London, EC4N 6AE

Data Controller Email: [dataservices@judicium.com](mailto:dataservices@judicium.com)

You have the right to make a complaint at any time to the Information Commissioner’s Office, the UK supervisory authority for data protection issues.

**Appendix 5 – Management Instructions to Employees Issued Summer 2018**

In the light of legislation effective from 25th May 2018, the following must be considered management instructions in order to protect you and your colleagues.

1. Printing to photocopiers must be done through the 'Locked' or 'Secure' print' setting (i.e. can only be activated by a PIN on arrival at the machine). To do this you will need to access the 'Printer Properties' button and change to one of the above settings.
2. Personal data relating to pupils (e.g. DoB/assessment information) should not be on display. Data relating to families (e.g. correspondence with addresses or telephone numbers) should not be displayed or be easily accessible.
3. We have clear screen (computers logged off when not attended) and clear desk (none of the above data is on display or easily obtained) policies in place.
4. Emails must not contain names of specific pupils although initials are acceptable. If further information about a child needs to be sent to a colleague, use a password-protected attachment.
5. Memory sticks to transport data to/from work are not permitted. Google Drive is your point of access if working on school documents off site.
6. School devices (laptops/ipads) must not be used for any personal purpose. We have monitoring software in place that will pick this up if it is happening.
7. If you are using a personal mobile phone on the premises, school wifi must not be used to access any websites that are not work-related. If something does need to be accessed for personal reasons, you must switch to 3G or 4G. Monitoring software will also pick this up.
8. You must log-off PCs when not using them for an extended amount of time. PCs that have remained idle for 20 minutes between the hours of 5.00pm and 7.30am will be logged off automatically.

These are very important instructions to follow. One of the changes caused by the act is the mechanism to prosecute individuals if there is a data breach/loss. If this occurs and it is proved that an employee has chosen not to follow instructions issued to them, liability passes to the individual. Following the above will protect you from this.

Technicians are available to help and support you with any of the detail described above. They are in every Monday (between 1pm and 4pm) and every Wednesday (between 10am and 1pm). Alternatively, contact them at [helpdesk@stmryb29.bham.sch.uk](mailto:helpdesk@stmryb29.bham.sch.uk)