St Peter's Bratton Church of England Academy

Data Protection

Data Protection Policy- Document Status			
Date of Policy Creation	March 2019	**Named Responsibility**	Governing Body
Reviewed	March 2022	**Named Responsibility**	Principal
Next Review Due	March 2024	**Named Responsibility**	Principal

1. Introduction

The Data Protection Act 2018 (DPA 18) / General Data Protection Regulations (GDPR) defines UK law on the processing of data on identifiable living people. It is the main piece of legislation that governs the protection of personal data in the UK. Personal information is information about a living individual, who can be identified from the information.

1.1 St Peter's Bratton Church of England Academy is committed to protecting the privacy of individuals and handles all personal information in a manner that complies with the DPA18/GDPR. It is the **personal responsibility** of all employees (temporary or permanent), Local Academy Committee, contractors, agents and anyone else processing information on our behalf to comply with this policy.

1.2 Any deliberate breach of this policy could amount to a criminal offence under one or more pieces of legislation, for example the Computer Misuse Act 1990 and the DPA18/GDPR. All breaches will be investigated and appropriate action taken.

1.3 This policy explains what the School's expectations are when processing personal information and should be read in conjunction with the School Information Security Policy (SISP) – found at the end of this document.

2. GDPR Principles

2.1 The DPA18/GDPR is supported by a set of 6 principles which must be adhered to whenever personal information is processed. Processing includes obtaining, recording, using, holding, disclosing and deleting personal information.

2.2 The DPA 18/GDPR principles relevant to the school state that personal information must:

Be processed fairly, lawfully and transparently	**Obtained for a specified, explicit and legitimate purpose**	**Be adequate, relevant and limited to what is necessary**
Be accurate and where necessary up to date	Not be kept longer than is necessary	Be handled ensuring appropriate security

3. Access and Use of Personal Information

3.1 Access and use of personal information held by the school, is only permitted by employees (temporary or permanent), Local Academy Committee, contractors, agents and anyone else processing information on our behalf, for the purpose of carrying out their official duties. Use or access for any other purpose is not allowed. Deliberate

unauthorised use and access to copying, destruction or alteration of or interference with any personal information is strictly forbidden.

4. Collecting Personal Information

4.1 When personal information is collected, for example on a questionnaire, survey or an application form, the 'data subject' (that is the person who the information is about) must be told. This is known as a Privacy Notice.

4.2 Personal information collected, must be adequate, relevant and not excessive for the purpose of the collection. A person's name and other identifying information should not be collected where anonymous information would suffice.

4.3 If the information is collected for one purpose, it cannot then be used for a different and unconnected purpose without the data subject's consent unless there is another lawful basis for using the information (see section 5 below). It must be made clear to the 'data subject' all the purposes that their information may be used for **at the time the information is collected**.

5. Lawful Basis for Processing

5.1 When St Peter's Bratton Church of England Academy processes personal information, it must have a lawful basis for doing so. DPA18/GDPR provides a list of 'conditions' when we can process personal or 'special category' personal information. This is contained within Article 6 and Article 9 of the regulations ***(see Appendix 1)***.

5.2 The DPA18/GDPR defines special category personal information as information relating to:

- Race and ethnic origin
- political opinion
- religious or philosophical beliefs
- trade union membership
- processing of genetic/biometric data to uniquely identifying a person
- physical or mental health or medical condition;
- sexual life

5.3 Whenever the School processes personal information, it must be able to satisfy at least one of the conditions in Article 6 of the GDPR and when it processes 'special category' personal information; it must be able to satisfy at least one of the conditions in Article 9 of the GDPR as well.

5.4 The School can process personal information if it has the data subject's consent (this needs to be 'explicit' when it processes sensitive personal information). In order for consent to be valid it must be 'fully informed' which means the person giving consent must understand what they are consenting to and what the consequences are if they give or refuse consent. Consent must not be obtained through coercion or under duress and should be recorded.

6. Disclosing Personal Information

6.1 Personal information must not be given to anyone internally or externally, unless the person giving the information is fully satisfied that the enquirer or recipient is authorised in all respects and is legally entitled to the information.

6.2 If personal information is given to another organisation or person outside of the School, the disclosing person must identify the lawful basis for the disclosure (see section 4 above) and record their reasoning for using this basis. This record as a minimum should include;

- a description of the information given;
- the name of the person and organisation the information was given to;
- the date;
- the reason for the information being given; and
- the lawful basis.

6.3 If an information sharing agreement or protocol exists, this should be adhered to when providing personal information to others. The agreement/protocol will provide the legal basis for disclosure.

6.4 In response to any lawful request, only the minimum amount of personal information should be given. The person giving the information should make sure that the information is adequate for the purpose, relevant and not excessive.

6.5 When personal information is given either externally or internally, it must be communicated in a secure manner, e.g. password protected emails, special delivery or courier, etc. For internal communications either hand deliver or make sure you email the information to the correct recipient.

7. Accuracy and Relevance

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

7.2 ‘Data subjects’ have a right to access personal information held about them and have errors corrected. More information about a ‘data subject’s’ rights can be found in Section 9 of this policy.

8. Retention and Disposal of Information

8.1 St Peter’s Bratton Church of England Academy holds personal information. The DPA18/GDPR requires that we do not keep personal information for any longer than is necessary. Personal information should be checked at regular intervals and deleted or destroyed securely when it is no longer needed, provided there is no legal or other reason for holding it.

8.2 The Information Retention scheldue must be checked before records are disposed of, to make sure that the prescribed retention period for that type of record is complied with. Alternatively advice should be sought from the schools Data Protection Officer.

9. Individuals Rights

9.1 Individuals have a number of rights under DPA18/GDPR. These include:

- **The right to be informed** – See section 4 - Collecting Personal Information
- **The right to access** – A person can ask for a copy of personal information held about them (this is known as a Subject Access request - SAR);
- **The right to rectification** – Personal data can be rectified if it is inaccurate or incomplete
- **The right to erasure** – Person can ask for the deletion or removal of personal data where there is no reason for its continued processing
- **The right to restrict processing** – Person has the right to block or suppress processing of their personal data
- **The right of data portability** – Allows a person to obtain and reuse their personal data for their own purposes
- **The right to object** – A person can object to an organisation processing their personal data for direct marketing, on the basis of legitimate interests or for scientific/historical reseach and statistics
- **Rights related to automated decision making/profiling** – A person can ask for human intervention in an automated process

9.2 If the school receives such a request on any of the above matters they should seek advice from their Data Protection Officer. Relevant people can be accecessed in our privacy statement.

9.3 The School has one calendar month in which to respond to a SAR, provided the applicant has put their request in writing by completing a subject access request form and suitable proof of identification has been supplied. An extension of a further 1-2 months will be applied where a request is deemed complex The School co-ordinates the processing of all SAR requests. ***See Appendix 2*** for a copy of the SAR form

10. Reporting Security Incidents

10.1 The School has a responsibility to monitor all incidents that occur within the organisation that may breach the security and/or the confidentiality of its information. All incidents need to be identified, reported, investigated and monitored. It is only by adopting this approach that the School can learn from its mistakes and prevent losses recurring.

10.2 Specific procedures have been developed for the reporting of all information security incidents. It is designed to make sure that all relevant information is communicated correctly so that timely corrective action can be taken. The documents below need to be read, understood and followed:

- Information Security Breach Procedure
- Data Breach Investigation

10.3 All employees (permanent, temporary and contractors) must be aware of the procedures and obligations in place for reporting the different types of incidents which may have an impact on the security of the Schooll’s information.

Article 6 Conditions – Personal Data

(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary in order to protect the vital interests of the data subject;
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. **This shall not apply to processing carried out by public authorities in the performance of their tasks.**

Article 9 Conditions – Special Category Data

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
(e) processing relates to personal data which are manifestly made public by the data subject;
(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Appendix 2

General Data Protection Regulations
Right of Access to Personal Data

SUBJECT ACCESS REQUEST FORM

Information

We should respond to your request within one calendar month. Note this can be extended for a further 2 months if the request is deemed complex. However this period does not start until:

a) We are satisfied about your identity
b) You have provided enough detail to locate the information you are seeking

Please complete the following sections of this form providing as much information as possible to help us deal with your request.

1. Provide details of the person about whom the School is holding data (the Data Subject)

Full Name (Print) _____

Date of Birth _____

Present Address:	Previous Address (if less than 3 years at your present address):
Post Code:	Post Code:

Telephone Number _____

Email address _____

2. Are you requesting information about yourself (person referred to in question 1)? If **YES**, then go to question 3. If **NO** please complete the following:

Full Name (Print) _____

Present Address:

Post Code:

Telephone Number: _____

Email address: _____

Relationship with data subject and brief explanation as to why you are requesting this information rather than the data subject:

_____

_____

If you are acting on behalf of the data subject you will need to enclose their written authority including a signature or other legal documentation (e.g. power of attorney) to confirm this request. You also need to enclose evidence of your identity and that of the data subject (see section 4 for details of acceptable identity)

3. Please provide a clear description of the information that you are requesting, see table below. **If you provide <u>specific</u> details of what information you want, e.g. name of a document relevant to a time period rather than just the whole of your file you may receive a quicker response.**

Description of Information	School Holding this Information	Time Period for Information Requested

4. Please provide **two** pieces of evidence of your identity (one containing a photo). Acceptable types of documents used to verify your identity are detailed below.

Driving Licence	Passport	National ID Card	Medical Card	Utility Bill

You may wish to send your documents special/recorded delivery. Your proof of identity will be returned to you securely after verification.

5. All information in respect to your request will be sent to you via secure email unless alternative arrangements are made. We may require further evidence of your identity if you collect your information from School premises.

Declaration

To be completed by all applicants. Please note that any attempt to mislead the School may lead to prosecution.

I (insert name) _____

_____

certify that the information given on this application form and any attachments therein to St Peter's Bratton Church of England Academy is accurate and true.

I understand that it is necessary for St Peter's Bratton Church of England Academy to confirm my identity and it may be necessary to obtain more information in order to locate the correct information.

Signature _____

Date _____

Return of the Form

If you are either posting your documents or hand delivering them then our address is detailed below:

St Peter's Bratton Church of England Academy
Squirrel Meadow
Bratton
Telford
TF5 0NT

Our email address is stpeterrsbratton@taw.org.uk

How we will send you the information you have requested

We want you to receive the information you have requested in the most convenient way for you.

However we do have an obligation under the General Data Protection Regulations to provide you with the information you have requested in the most secure way possible.

We believe the most secure way to provide you with the information is either:

- For you to collect the documentation in person from our offices
- For us to email you the information securely/encrypted

We can post your information to you but there are risks attached to providing you with your information using this method, e.g. Royal Mail may lose your information, deliver it to the wrong address, etc.

Please confirm you are happy to receive your information by secure email by ticking the box below and confirming the email address that your information should be sent to:

Tick Box		EMAIL ADDRESS	

Alternatively if you prefer any of the other methods below please indicate which by ticking ONE of the boxes below:

Collection in person		CD or Paper Copy *(please circle your choice)*
By Post (special delivery)		CD or Paper Copy *(please circle your choice)*

SCHOOLS INFORMATION SECURITY POLICY

'Information security is everyone's responsibility'

1. Why do we need security?

Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post, email, and even spoken in conversations.

The purpose of information security is to ensure that all information (including personal information) and associated processing systems are protected to an adequate level from events that may cause personal distress or have a negative impact on the School and its services.

This policy promotes good practices in respect to information security ensuring 3 main principles are embedded in the authorities' manual/electronic records management systems:

Confidentiality	Integrity	Availability
Information only accessed by authorised individuals	Safeguards accuracy and completeness of information	Ensure authorised officers have access when needed

Information security is not all about protecting the School from financial penalties it is about respecting the lives and rights of the residents/partners in our community and our employees.

2. Lost Information

You should always report any instances of lost personal information or where it has been sent to the wrong person(s) immediately to the Head Teacher so the risks and impacts can be properly managed. Do not forget information security concerns many things including letters, reports, emails, paper files, etc, but can also include issues such as lost laptops, work mobile phones, lost digital cameras, lost memory sticks, etc. See the Information Security Breach Procedure (ISBP) in the staff handbook.

3. Sharing Information

What should a School officer consider when asked to share personal identifiable information (PII) with other third parties?

- Only share PII if you have the legal justification to do so
- Share information in compliance with the SISP and Information Sharing Policy
- Know the objective/reasons for sharing PII
- Investigate whether the objective can be met another way without sharing PII
- Send elements of PII that are definitely required to meet the objective/reasons
- Where possible, anonymise the information you send so it is not personally identifiable
- Confirm the recipients contact details before sharing information
- Appropriately protect the PII you are sharing by either using encryption / password if it is electronic, by using special delivery if posting, etc.

4. Sensitive Information

The School handles numerous types of sensitive data on a day-to-day basis. The following are a list of do's and don'ts in respect to handling sensitive data.

Do's	Don'ts
If you lose any sensitive or personal information then this should be reported immediately to your Head Teacher	Do not store sensitive or personal information on portable media (laptops, memory sticks, CD's, etc) unless in very exceptional circumstances and when the media is encrypted
When discussing sensitive or personal information on the phone consider who may be listening in at both ends of the phone line	Do not give out sensitive information unless the person is authorised to receive it and the data owner has approved that you can send it
Understand your responsibilities under the Data Protection Act 2018 and full version of the School Information Security Policy (SISP).	Do not leave sensitive or personal information on printers, computer screens or desks whilst away from your desk
Keep sensitive information stored securely and restrict access on a need to access basis	Do not access any sensitive or personal information that is not relevant to your role
Ensure that sensitive data, both paper based and electronic are shredded / disposed of correctly	

5. Passwords

It is your responsibility as a user to:

- Do not share passwords
- If you think someone is aware of your password change it straight away
- Avoid writing down passwords
- Make passwords hard to guess; try to avoid using family names.
- Ensure your password includes upper and lower case letters, numbers and a special character (not a number or letter, e.g. an exclamation mark)
- Change your password every 3 months or when prompted to do so.

6. Email/Other Communication Technologies (OCT)

See full copy of SISP for what is defined as reasonable use of email/OCT. Appropriate use includes:

- Email/OCT (private on School equipment) must not contain indecent, inappropriate or offensive content
- Take care when addressing email messages to ensure a correct address is used
- Do not send personal or sensitive information via unprotected email
- Reasonable personal use is allowed in non-work time only
- Do not take part in chain letter emails

7. Internet

You should always remember that your School internet access is primarily provided for business use. See full copy of SISP for what is defined as reasonable use of the internet. Please note:

- All internet use on School equipment is logged for management purposes
- Reasonable personal use is permitted in non-work time
- Do not use the School's internet (both within and outside working hours) to access inappropriate, offensive, illegal or adult/sexually explicit material. A full list of types of website that are unauthorised is detailed in the full version of the SISP
- Do not leave the internet logged on when you leave your computer unattended

8. SISP – Summary of Key Messages to Employees

YOU MUST:

- Ensure you take steps to safeguard the security of information you hold/access
- Comply with the SISP, associated acceptable use policies and the information breach procedure
- If you handle personal information, have an adequate awareness of your Data Protection Act/GDPR responsibilities
- Report lost/stolen ICT equipment/personal information to your Head Teacher
- Complete information governance training
- Only share personal information if there is legal justification to do so
- Where possible anonymise personal information shared with non-School parties, e.g. use a reference number and not a name
- Appropriately protect information that is being shared
- Confirm the recipients details, e.g. email address, location, etc. before sharing the information
- Only access information/systems that you need to undertake your duties
- Use secure passwords and never share them with your colleagues
- Direct external parties that need access to the School's network to the ICT Technician
- Lock down your pc/laptop when you leave it unattended for a prolonged period
- Be responsible for the physical security of School ICT equipment and information in your possession (i.e. paper files) making sure that these are securely stored
- Ensure your mobile device has PIN security activated
- Only use USB sticks or other removable media (e.g. external hard drives, digital cameras, etc) on an exception basis and only use those that are encrypted
- Ensure information held on removable media is encrypted/password protected
- If you are mobile/home worker, ensure that ICT equipment and information used on the road or at home, is locked down/away securely when not in use
- Never leave ICT equipment and/or personal information in a car overnight
- Do not use email on School equipment/networks for personal use in works time
- Only use the internet for personal use in non-work time
- Undertake a data protection impact assessment on all new/developed ICT systems that involve processing/viewing of personal information