ST GEORGE'S CHURCH OF ENGLAND FOUNDATION SCHOOL

"Every moment, every day, every individual counts"

DATA PROTECTION AND SUBJECT ACCESS REQUESTS POLICY

Last Reviewed: ***July 2020***

Due for Review: ***July 2021***

Governors Monitoring Pair:	Leadership and Management
SLT Responsible:	Headteacher
Review Period:	Annually

DATA PROTECTION POLICY

Contents:

1. AIMS:

St George's Church of England Foundation School aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (EU() 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018).

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

2. LEGISLATION AND GUIDANCE:

This policy meets the requirements of the GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR.

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

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

3. DEFINITIONS:

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.

Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. THE DATA CONTROLLER:

St George's Church of England Foundation School processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

St George's School has an external Data Protection Officer.

5. ROLES AND RESPONSIBILITIES:

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

5.1 Governing Board:

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

5.2 Data Protection Officer:

The school has an external Data Protection Officer, who liaises with the school Data Protection Lead. The Data Protection Lead is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

The DPO is also the first point of contact, via Liz Burden (Data Protection Lead), for individuals whose data the school processes, and for the ICO.

Our DPO is contactable via Liz Burden (Director of Finance and Data Protection Lead) 01843 861696.

5.3 Headteacher:

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

5.4 All staff:

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO, via Liz Burden, in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - If they have any concerns that this policy is not being followed
  - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
  - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
  - If there has been a data breach

- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

6. DATA PROTECTION PRINCIPLES:

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

7. COLLECTING PERSONAL DATA:

7.1 Lawfulness, fairness and transparency:

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

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

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent when appropriate in the case of a pupil) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes,** and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentially under law

- The data needs to be processed for **public health reasons** and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentially under law
- The data needs to be processed for **archiving purposes,** scientific or historical research purposes, or statistical purposes and the processing is in the public interest

For criminal offense data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent when appropriate in the case of a pupil) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in conjunction with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

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

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

7.2 Limitation, minimisation and accuracy:

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

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

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

We will keep data accurate and, where necessary, up to date. In accurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule. The School follows the "Information, Management Toolkit" for Schools Guidance document.

8. SHARING PERSONAL DATA:

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

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

- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data internationally, we will do so in accordance with the data protection law.

9. SUBJECT ACCESS REQUESTS AND OTHER RIGHTS OF INDIVIDUALS:

A request for access to data by a living person under the Act is known as a Subject Access Request or SAR. All records that contain the personal data of the subject will be made available, subject to certain exemptions.

9.1 Subject access requests:

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

Subject access requests must be submitted on the Subject Access Request Form (Appendix 2) to the Headteacher, and include:

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

If staff receive a subject access request in any form they must immediately forward it to the Data Protection Lead.

9.2 Children and subject access requests:

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

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Education Law will also be taken into account when requests are made.

9.3 Responding to subject access requests:

When responding to requests, we:

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

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

Where someone wants to see a small part of their data (an exam result or written consent), a formal SAR is not required if the individual can prove their identity, the information is readily available there and then, and no other third party data will be unreasonably released. Such requests should be dealt with quickly, as business as usual and with little formality.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

9.4 Other data protection rights of the individual:

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (ie, making decisions or evaluating certain things about an individual based on their potential data with no human involvement)
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

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

9.5 Compliance to release of data:

Before a SAR is sent out to the data subject the Headteacher or their nominated representative(s) is / are required to carry out a review of the data to be released. This is done to ensure that all third party data has been removed appropriately and that any documents have been redacted appropriately.

Third party data sent out in error to the wrong person constitutes a data breach under the Data Protection Act 2018 and can have very serious consequences for the school.

Where the redaction of SARs is outsourced to a third party provider a review of the work completed must be carried out by the Headteacher or their nominated representative(s) before any documents are sent out to the data subject. This is to ensure that the work is completed to the standards expected by the school.

9.6 Responding to a SAR:

Once all of the information has been collated (duplicates and third party information has been removed or redacted and a double check has been carried out) the information will be provided either in paper copy, electronically or during a meeting with the Data Subject and sent securely. The school is required to provide the copies in a format requested by the data subject.

9.7 Complaints:

The school will provide a right of complaint to all applicants in the event they are dissatisfied with the handling of their request. If an applicant is unhappy with the service they have received they should contact the Headteacher.

If the applicant is dissatisfied with the content of the information they have received they should also make a complaint in writing to the Headteacher. If an applicant remains dissatisfied with the outcome of their complaint, advice will be sought from the school's Data Protection Lead via the DPO. The Data Protection Officer will make an independent assessment of the case and notify their findings to the Headteacher who may amend the content of the information previously issued. If the applicant remains dissatisfied they may ask the Information Commissioners Office to carry out an independent investigation.

9.8 Appealing a decision to refuse disclosure of Information:

If the school refuses to disclose information in response to a subject access request, the school will offer the applicant an opportunity to appeal the initial decision. Once an appeal has been received the Headteacher will conduct an internal review and the applicant advised of the outcome within 20 working days.

If an applicant's appeal is successful they will receive the information they requested as soon as possible. If the appeal is unsuccessful the school will provide a detailed explanation of the findings and supply further information on how to take the matter further.

9.9 Complaining to the Information Commissioners Office:

If an applicant is not satisfied with the outcomes of the schools decisions they have the right to submit a complaint to the Information Commissioners Office. The Information Commissioners Office will make an initial assessment of the case before carrying out an investigation.

The Information Commissioners Office has written guidance notes for applicants on how to complain to the Information Commissioners Office and published it on their website, www.ico.gov.uk

9.9 Related documents:

- Freedom of Information Policy

9.10 Parental requests to see the educational record:

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

This right applies as long as the pupil concerned is under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

10. CCTV:

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

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

Any enquiries about the CCTV system should be directed to the School's Director of Finance.

11. PHOTOGRAPHS AND VIDEOS:

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

Primary School:

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

Any photographs and videos taken by parents at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents have agreed to this.

Secondary School:
We will obtain written consent from parents, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Any photographs and videos taken by parents at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents (or pupils where appropriate) have agreed to this.

Where the school takes photographs and videos, uses may include:

- Within school on notice boards and in prospectus and newsletters, etc
- Outside of school by external agencies such as the school photographer, newspapers
- Online on our school website or social media pages

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

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

See our Safeguarding and Child Protection Policy for more information on our use of photographs and videos.

12. DATA PROTECTION BY DESIGN AND DEFAULT:

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

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the European Economic Area (EEA) where different data protection laws will apply

- Maintaining records of our processing activities, including:
  - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
  - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipient, any transfers outside of the EEA and the safeguards for those, retention periods and how we are keeping the data secure.

13. DATA SECURITY AND STORAGE OF RECORDS:

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

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our Online Safety, Acceptable Use and Acceptable Use Policy).
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).

14. DISPOSAL OF RECORDS:

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law. The school follows the "Information Management Toolkit" document for school guidance for retention.

15. PERSONAL DATA BREACHES:

The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1. When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

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

16. TRAINING:

All staff and governors are provided with data protection training as part of their induction process.

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

17. MONITORING ARRANGEMENTS:

The Data Protection Lead is responsible for monitoring and reviewing this Policy. This policy will be reviewed annually and shared with the full Governing Board.

18. LINKS WITH OTHER POLICIES:

This data protection policy is linked to our:

- Freedom of information Policy
- Online Safety, Acceptable Use Policy
- Safeguarding and Child Protection Policy

Appendix 1: Personal data breach procedure

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

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

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school Network.

- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through their breach report line (0303 123 1113), within 72 hours. As required, the DPO will set out:
  - A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - A description, in clear and plain language, or the nature of the personal data breach
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

As above any decision on whether to contact individuals will be documented by the DPO.

- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts relating to the breach
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the school's network.

- The DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

ST GEORGE'S CHURCH OF ENGLAND FOUNDATION SCHOOL

SUBJECT ACCESS REQUEST FORM

Dear St George's Church of England Foundation School

Please provide me with the information about me that I am entitled to under the General Data Protection Regulation. This is so I can be aware of the information you are processing about me, and verify the lawfulness of the processing.

Here is the necessary information:

Name (Pupil name if applicable):	
Relationship with the school:	***Please select:*** Pupil/parent/employee/governor/volunteer Other (please specify):
Correspondence Address:	
Contact Number:	
Email Address:	
Details of the information requested	***Please provide me with:*** Insert details of the information you want that will help us to locate the specific information. Please be as precise as possible, for example: • My personnel file • My child's medical records • My child's behaviour record

If you need any more information from me, please let me know as soon as possible. Please bear in mind that, in most cases, you must supply me with the information within 1 month and free of charge.

SIGNED:_____ **NAME:**_____