St John's Church of England Primary School

UK GDPR and Data Protection Policy

And you will feel secure, because there is hope;
you will look around and take your rest in security.
Job 11.18

Date agreed and ratified by Governing Body: July 2023

Date of next review: July 2024

1. Aims

The school aims to ensure that all personal data collected about staff, pupils, parents, governors, school, members, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and statutory guidance by all establishments in the organisation. All establishments in the organisation are referred to as the 'School' in this policy.

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 is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

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

In addition, this policy complies with the School's funding agreement and articles of association.

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 • Sexual orientation • Gender
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

The school processes personal data relating to individuals, and therefore is a data controller.

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

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

5.1 Governing Body

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

5.2 Data protection officer

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

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

The School's DPO is Satswana Ltd, info@satswana.com; telephone number 01252 516898.

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

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 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 the 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

7. Collecting personal data
7.1 Lawfulness, fairness and transparency
The School will only process personal data where there is one of 6 'lawful bases' (legal reasons) to do so under data protection law:

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

For special categories of personal data, the School will also meet one of the special category conditions for processing which are set out in the GDPR.

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

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

7.2 Limitation, minimisation and accuracy
The School will only collect personal data for specified, explicit and legitimate reasons. The School will explain these reasons to the individuals when data is collected.
If the School wants to use personal data for reasons other than those given when first obtained, it will inform the individuals concerned before it does so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

8. Sharing personal data
The School will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of staff or pupils at risk
- The need to liaise with other agencies
- The School's suppliers or contractors need data to enable the School to provide services to staff and pupils – for example, IT companies. When doing this, the School 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 shared

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

The School will also share personal data with law enforcement and government bodies where it is legally required to do so, including for:

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

The School may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects pupils or staff.

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

9. Subject access requests and other rights of individuals

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
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted by email to the DPO. They should include:

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

If staff receive a subject access request they must immediately forward it to the DPO. Staff need to be aware that a subject access request may arrive in different formats.

9.2 Responding to subject access requests

When responding to requests, the DPO:

- Will ask the individual to provide 2 forms of identification, including photo identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual the School will comply within 3 months of receipt of the request, where a request is complex or numerous.

The School will not disclose information if it:

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

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

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

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

9.3 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 the School are collecting their data about it is used and processed (see section 7), individuals also have the right to:

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

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

10. CCTV

The School uses CCTV in various locations around its sites to ensure it remains safe. The School does not need to ask individuals' permission to use CCTV. Any enquiries about the CCTV system should be directed to the Headteacher in the first instance.

11. Photographs and videos

As part of school activities, photographs and record images of individuals within the establishments may be taken.

The School will obtain written consent from parents/carers for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where the School needs parental consent, it will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within school on notice boards and in School magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on the establishment and School websites or social media pages

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

When using photographs and videos in this way no personal information about the child will be given, to ensure they cannot be identified.

12. Data protection by design and default

The School will put measures in place to show that data protection is integrated into all 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; keeping a record of attendance
- Regularly conducting reviews and audits to test privacy measures and make sure the School is compliant
- Maintaining records of processing activities, including:

- For the benefit of data subjects, making available the name and contact details of our School and DPO and all information the School is required to share, about how personal data is processed (via privacy notices)
- For all personal data held, maintaining an internal record of the type of data, data subject, how and why the data is used, any third-party recipients, how and why the data is stored, retention periods and how the data is kept safe

13. Data security and storage of records

The School 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. Appropriate organisational and technical steps will be taken to secure data.
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
- Passwords are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- 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
- Where personal data is shared with a third party, the School will 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.

Paper-based records will be shredded, and electronic files will be deleted. The School may also use a third party to safely dispose of records on the school's behalf. The third party is required to provide sufficient guarantees that it complies with data protection law.

15. Personal data breaches

The School will make all reasonable endeavours to ensure that there are no personal data breaches.

In the event of a suspected data breach, the procedure set out in appendix 1 will be followed.

When appropriate, the data breach will be reported to the ICO within 72 hours by the DPO. 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

Staff are provided with annual data protection reminders. 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 School's Data Protection Manager is responsible for monitoring and reviewing this policy and for working with the DPO.

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 DPO: Satswana Ltd, info@satswana.com; telephone number 01252 516898.

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

  If it is 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 provided to the Data Protection Manager.
- Where the ICO must be notified, the DPO will do this within 72 hours. As required, the DPO will set out:

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

  Records of all breaches will be stored.
- The DPO, Data Protection Manager and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

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

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it.
- In any cases where the recall is unsuccessful, the Headteacher will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.
- The DPO will carry out an internet search to check that the information has not been made public; if it has, the School will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

Other types of breach could include:

- Details of pupil premium interventions for named children being published on the school website.
- Non-anonymised pupil exam results or staff pay information being shared with governors.
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked.