Data Protection Policy

Including Data Security provisions

This School is committed to safeguarding and promoting the welfare of children and young people and expects all staff, governors and volunteers to share this commitment.

Last reviewed: May 2024

Next review due: May 2026

ST PETER'S C of E INFANT SCHOOL DATA PROTECTION POLICY

Contents

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the 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 DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

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, living individual. It does not include anonymised data or data from which no individual is capable of being identified. Personal data may include the individual's: • Name (including initials) • Identification number • Location data (e.g. address/contact details) • 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 / Sensitive 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

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, 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.

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

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 and Data Protection Lead

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

They will provide regular updates of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues. Please contact the school office for details of the Data Protection Officer.

The school also has a Data Protection Lead (DPL) who is responsible for the day to day management and implementation of this policy and is the first point of contact for individuals whose data the school processes. The current DPL is the School Business Manager.

5.3 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
- In the first instance, contacting the DPL 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,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

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

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

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

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. Inaccurate data will be rectified or erased when appropriate.

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 *Information and Records Management Society's toolkit for schools*

8. Sharing personal data

We will not normally share personal data with anyone else unless we have consent to do so. Exceptions to this are:

- If there is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- If we need to liaise with other statutory agencies as part of the official educational requirements of the school
- 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, 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
- 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 to a country or territory outside the European Economic Area, we 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 should be submitted in writing, either by letter, email or fax to the DPL. 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 DPL. The DPL should also inform the DPO.

9.2 *Children and subject access requests*

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

Children below the age of 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 or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

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

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- 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
-

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

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

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

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:

- Under certain circumstances, withdraw their consent to processing and/or challenge processing which has been justified on a basis other than consent
- Ask us to rectify their personal data
- Prevent use of their personal data for direct marketing
- If applicable, to request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Challenge decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them) if such processes are used
- 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 DPL. If staff receive such a request, they must immediately forward it to the DPL. The DPL should also inform the DPO

10. Parental requests to see the educational record

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

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.

11. Photographs and videos

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

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

will be used to both the parent/carer and pupil.

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

Uses may include:

- Within school on notice boards, wall displays, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, etc.
- Online on our school website and in the school prospectus.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video wherever possible 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 Use of Photographic Images 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 ensure that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitable DPO
- 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)
- Integrating data protection into internal documents and procedures
- Regularly training members of staff on data protection, this policy, any related policies and any other data protection matters
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant

Maintaining appropriate records of our processing activities

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.

All staff must comply with the following data security principles:

<u>General</u>

- Only people who are authorised to use school personal data may access it.
- All school systems (SharePoint cloud storage, school email accounts, school computers and network) shall be controlled by individual passwords. These are unique to each individual and must never be given to anyone else.
- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data shall be kept under lock and key when not in use

<u>Passwords</u>

- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops, and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Passwords to access school systems should never be shared with someone else. Passwords should never be displayed nor stored on or with a computer.

Personal devices

- Any personal device used for school business by a member of staff or volunteer must be password protected and have up-to-date virus protection software installed.
- No Personal data should be *stored* on any non-school devices i.e. personal devices owned by staff/volunteers. All such data should be stored on the school's cloud-storage systems and accessed from there if required.
- Any data downloaded onto a personal computer in the normal course of work must be deleted as soon as it has been dealt with – this should include emptying any 'recycle bin'. Care must be taken to regularly clear temporary computer files of all files containing personal data.

Emails

- Staff should only ever use official school email accounts to correspond with third parties on school related matters.
- Emails containing personal data should be regularly deleted. No emails containing personal data should be kept for longer than necessary.
- If school-related personal data is received into a personal email account (i.e. non-school account) of any school staff or volunteer, it should be deleted as soon as practicable. Correspondence containing school-related personal data should never be *stored* on non-school email accounts.

Paper records

- No paper records shall be taken off school premises apart from in exceptional circumstances as authorized by the Head Teacher (this does not apply to marking of schoolwork containing minimal personal data, in the normal course of the school's activities). The school will not permit paper copies of contact details to be taken off school premises.
- Any authorised paper records of personal data taken externally should only be kept temporarily whilst they are being worked. The paper record should then be returned immediately to source or securely destroyed (shredded) as appropriate.
- Papers containing 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

Sharing personal data

- Personal data should only ever be shared with people who have been authorised to receive it, and only for the purposes for which such data was intended.
- Personal data should be shared between staff/volunteers by saving it to and retrieving it from the school's secure cloud-storage. Data should only be transferred in other ways (e.g. to a non-school email, or removable storage) if it is essential to do so. Any data transferred in this way must be suitably encrypted (e.g. password protected) or have other data protection measures in place so that if the data is lost, stolen, or subject to unauthorised access, it remains secure.

15 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.

16. 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

17. 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.

18. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed **every 2 years** and shared with the full governing board.

19. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Use of Photographic Images Policy
- Privacy Notices
- E-Safety 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 DPL
- The DPL will investigate the report and determine whether a breach has occurred. To decide, the DPL 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 DPL will immediately alert the DPO, headteacher and the chair of governors
- The DPL and 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. 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 based on the appropriate guidance issued by the ICO. This will be judged on a case-by-case basis and appropriate records will be kept on any decisions reached.
- Where the ICO must be notified, the DPO will follow the appropriate ICO guidance on reporting.
- 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 DPL 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 DPL 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 DPL will document each breach on a central record, 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)
- 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.