ST. KATHARINE'S C.E. (V.A.) PRIMARY SCHOOL

Data Protection Policy

Reviewed by	Headteacher, SBM and DPO November 2025
Date Determined by Governing Body	Resources 3.12.25
Next review date	November 2026

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 UK General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

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:

1. UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
2. Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

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 (not including any child protection information)

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 (often referred to as a UPN) • Location data (including addresses) • 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

Data processing	Anything done to personal data, which includes but is not restricted to: 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.

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 body

The governors have overall responsibility for ensuring that our 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 our compliance with data protection law, and assisting us to develop related policies and guidelines where applicable.

They will provide a regular report to the school containing relevant updates and information and, where relevant, report to the governors their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for the ICO.

DPO – School Pro TLC Ltd, 01425 947633, dpo@schoolpro.uk

01202 482588

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

5.4 School's Data Protection Lead
Within the school the School Business Manager is responsible for monitoring compliance of this policy and our Privacy Notices on a daily basis. They will liaise regularly with the DPO when required, including with any concerns raised by others, and will ensure school staff are kept up to date and informed of updates and required actions.

The Data Protection lead is the first point of contact for individuals whose data the school processes.

Our Data Protection Lead is Tracey Deem office@skps.email FAO Data Protection Lead 01202 426663.

5.5 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 school's Data Protection Lead (who may then refer on to 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, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If they believe 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 UK 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:

1. 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
2. The data needs to be processed so that the school can **comply with a legal obligation**
3. The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life

4. 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
5. 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)
6. 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 UK GDPR and Data Protection Act 2018.

- The individual (or their parent/carer 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 confidentiality 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 confidentiality 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 offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer 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 connection 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. This is normally done through our Privacy Notices which are freely available on our school website.

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, normally via our Privacy Notices.

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, often by updating our privacy notice, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs. If in doubt they will refer to the school's Data Protection Lead.

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, but may do so where:

1. There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
2. We need to liaise with other agencies – consent is often necessary for this
3. 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:
    a) Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    b) Establish a UK 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
    c) 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
    d) Ensure data subjects (or their parents in the case of minors) are aware of these data sharing arrangements via our Privacy Notices

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 to a country or territory outside the European Economic Area, we will do so in accordance with UK 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
- 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 can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and 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 school's 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 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 2 forms of identification
- May contact the individual via phone or email to confirm the request was made
- May request a meeting with the individual to discuss the request in detail to allow us to provide the most suitable response
- 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 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

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 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 (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 (i.e. making decisions or evaluating certain things about an individual based on their personal 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 school's Data Protection Lead or the DPO. If staff receive such a request, they must immediately forward it to the school's Data Protection Lead.

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.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

This right applies as long as the pupil concerned is aged 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.

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, and consent will be sought for this.
At public events other parents may take photos of children – we always request parents do not share these on social media unless it is only of their own child.

Our uses of media may include:

1. Within school on notice boards and in school magazines, brochures, newsletters, etc.
2. Outside of school by external agencies such as the school photographer, newspapers, campaigns

3. Online on our school website or social media (Twitter and YouTube) pages
4. Display boards in classrooms

Consent can be refused or withdrawn at any time. If consent is withdrawn after a photo has been displayed, we will take every effort to 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.

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:

1. Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
2. Ensuring that the school's Data Protection Lead has the required resources and training to fulfil their duties and maintain their knowledge
3. 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)
4. 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)
5. Integrating data protection into internal documents including this policy, any related policies and privacy notices
6. 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/acceptance
7. Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
8. Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school's Data Protection Lead 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 recipients, how and why we are storing the data, 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 iPads 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, loose in staff pigeon holes, pinned to notice/display boards, or left anywhere else where there is general access
- Computers are to be locked when not in use using CTRL+ALT+DEL or WINDOWS+L as well as an auto lock facility if the computer is idle for 15 minutes
- Where personal information needs to be taken off site, staff must sign it in and out from the school office and take appropriate measures to ensure confidentiality

- Passwords are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to use complex passwords and change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as iPads
- Staff, pupils or governors who access personal information on their personal devices (for example via remote access) are expected to follow the same security procedures as for school-owned equipment (see our Online Safety 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 both paper-based and electronic records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with UK 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 unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, the data breach will be reported 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 iPad containing non-encrypted personal data about pupils

16. Training

All staff 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, alongside regular updates and reminders.

17. Monitoring arrangements

The data protection lead and headteacher are responsible for monitoring and reviewing this policy.
This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **annually** and shared with the full governing body.

Appendix 1: Personal data breach procedure
This procedure is based on guidance on personal data breaches produced *by the ICO.*

The school's Data Protection lead is the School Business Manager.

1. On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the school's Data Protection Lead, who will then make contact with the DPO.
2. The school's Data Protection Lead will assist the DPO in investigating the report, and determine whether a breach has occurred. To decide, they will consider whether personal data has been accidentally or unlawfully:
    a. Lost
    b. Stolen
    c. Destroyed
    d. Altered
    e. Disclosed or made available where it should not have been
    f. Made available to unauthorised people
3. Where the breach is considered serious they will alert the headteacher and the chair of governors
4. They 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)
5. They will assess the potential consequences, based on how serious they are, and how likely they are to happen
6. 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:
    a. Loss of control over their data
    b. Discrimination
    c. Identify theft or fraud
    d. Financial loss
    e. Unauthorised reversal of pseudonymisation (for example, key-coding)
    f. Damage to reputation
    g. Loss of confidentiality
    h. 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.
7. Both the school's Data Protection Lead and 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 DPO's secure computer network and GDPRiS (an online platform to help schools comply with GDPR). Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    a. A description of the nature of the personal data breach including, where possible:
        i. The categories and approximate number of individuals concerned
        ii. The categories and approximate number of personal data records concerned
    b. The name and contact details of the DPO
    c. A description of the likely consequences of the personal data breach
    d. 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

8. 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
9. 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 or the school's Data Protection Lead will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    a. The name and contact details of the DPO
    b. A description of the likely consequences of the personal data breach
    c. 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
10. The DPO and school's Data Protection Lead will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
11. The DPO and school's Data Protection Lead will both document every breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    a. Facts and cause
    b. Effects
    c. 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 DPO's secure computer system and GDPRiS. All breaches will be reviewed to assess what happened and how it can be stopped from happening again.

Actions to minimise the impact of data breaches

We 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. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed (including safeguarding records)

1. All teachers' use school PC's on site and secure remote access when off-site. Whilst teachers know that they are able to access remote access from family PC's they acknowledge that login details should never be saved on these machines meaning data can only be accessed by the staff member using their password.
2. All teachers understand that they are not allowed to use USB drives to transfer data. They have remote access and also have access to OneDrive for Business.
3. Staff are aware of the importance of putting iPads in a locked cupboard or drawer and not leaving them in plain sight. All staff iPads are set to erase all data if an incorrect password is repeatedly entered.
4. Staff are aware that whilst it is acceptable to take photos on their class camera/iPad, they should transfer photos to our school media server and remove them from the portable device as soon as possible.
5. Staff are aware that they should place any documentation containing personal data that doesn't need to be kept (such as old test papers or pupil records) in confidential waste, and any information that does need to be kept to comply with the data retention policy is held in the school office or archive room in a secure manner.
6. Paper copies of pupil files being transferred to other schools will be in sealed envelopes, marked private and confidential with the return address of the school displayed clearly on the envelope. Pupil records will be signed out and a list of pupil names will be kept at our school.
7. Safeguarding files are transferred separately to pupil records to comply with safeguarding regulations.

Sensitive information being disclosed via email (including safeguarding records)

1. Members of staff who send or receive personal data in error must alert the sender (where received) and the school's Data Protection Lead as soon as they become aware of the error
2. If the sender is unavailable or cannot recall the email for any reason, the school's Data Protection Lead will ask the IT Manager to recall it if possible
3. In any cases where the recall is unsuccessful, the school's Data Protection Lead or the DPO 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
4. They will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
5. They will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Website:

1. As our school website is managed internally, if there was a case where certain data was published inappropriately, it could be taken down immediately.

Contracts with third parties:

1. Within school we have contracts with a number of organisations to support us in running the school more efficiently. With each contract we have it in writing that they follow and implement all the necessary procedures to comply with UK GDPR. If a third party is unable to provide us with this information, we would not enter into a contract with them.