



Data Protection Policy Number 7a

Spring Term 2024

Aims and Principles

St Paul's Cathedral School is a Christian, co-educational community which holds to the values of love, justice, tolerance, respect, honesty, service and trust in its life and practice, to promote positive relationships throughout the school community and where the safety, welfare and emotional well-being of each child is of the utmost importance.

The school aims to instil a love of learning through a broad curriculum. It aims to give each pupil the opportunity to develop intellectually, socially, personally, physically, culturally and spiritually. All pupils are encouraged to work to the best of their ability and to achieve standards of excellence in all of their endeavours.

Through the corporate life of the school, and through good pastoral care, the school encourages the independence of the individual as well as mutual responsibility. It aims to make its pupils aware of the wider community, espouses the democratic process and encourages a close working relationship with parents and guardians.

Data Protection School Policy No.7a

1. Introduction

Since the School processes a wealth of data, including sensitive data, this policy is to be read and understood by all members of staff.

The school maintains a **Privacy Policy on the school website**. This explains to parents and pupils how the school processes personal information.

It is important that all members of the school community take active measures to ensure the protection of data. Effective measures for staff and pupils should be taken to remind personnel of their obligations.

This policy will be reviewed every 2 years by the SLT and when required for endorsement by the Finance and Resources Committee.

2. Aims

To ensure that all personal and school-related 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 (UK GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018).

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

3. Legislation & Guidance

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

4. Definitions

Term	Definition
Personal Data	Any information relating to an identified, or identifiable, individual. This may include the individual's: <ul style="list-style-type: none">• Name (including initials)• Identification number• Location data

	<ul style="list-style-type: none"> • Online identifier, such as a username <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</p>
Special categories of personal data	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none"> • 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	<p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.</p> <p>Processing can be automated or manual.</p>
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.

5. The Data Controller

The 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.

6. Roles & 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.

Governing Body

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

Data Protection Lead

The data protection officer (DPL) 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 reports (as required) of their activities directly to the governing body and, where relevant, report to the body their advice and recommendations on school data protection issues.

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

Full details of the DPL's responsibilities are set out in their job description.

Our DPL's contact details are below:

Steve Vickery

Bursar and Clerk to Governors

St Paul's Cathedral School | 2 New Change, London, EC4M 9AD | **Tel:** +44 20 7248 0282 | **Mob** 07702 260158

Email: svickery@spcs.london.sch.uk | **Web:** www.spcslondon.com

Head

The Head acts as the line manager of the data controller and DPL on a day-to-day basis.

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 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

7. 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.

8. Collecting Personal Data

a. 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 UK 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.

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.

9. 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/carer 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, 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.

10. Subject Access Requests and other Rights of Individuals

a. 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 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.

b. 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:

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.

Children aged 12 and above:

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 or carers 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.

c. 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

- 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 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, 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.

d. 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, 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
- 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 DPL. If staff receive such a request, they must immediately forward it to the DPL.

11. Parental requests to see Educational Record

Parents have a 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. The school may charge a fee for hard copies.

12. Biometric Recognition Systems

The School does not currently use any biometric data.

If and where the School uses pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

13. CCTV

The School may use CCTV in various locations around the school site to ensure it remains safe. If we use CCTV 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 Data Protection Officer (DPL)

14. Photographs & Videos

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

Pupils aged under 18 years of age

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 need parental consent, 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 and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- 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 Policy & Child Protection and for more information on our use of photographs and videos.

15. Data Protection by Design & 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 DPL, 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
- 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 DPL 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
- Maintaining records of our processing activities, including:
 - For the benefit of data subjects, making available the name and contact details of our school and DPL 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

16. Data Security & 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 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
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices where personal information is stored
- 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 E-Safety policy on acceptable use)
- 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

17. Data Processing

To ensure adequate security measures, the DLP and IT Manager will prepare a DPIA (Data Protection Impact Assessment) for the most important and sensitive data processing done by the school. Currently this comprises 3 main IT systems:

- ISAMS – pupil records and administration.
- CPOMS – child protection information.
- Pass Finance – school financial information

Appendix 2 sets out the format of the DPIA.

18. Disposal of Records

The Retention of Data / Docs Policy is number 56 and has more specific information. 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.

19. 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

20. Training

All staff and governors are provided with data protection training as part of their induction process and thereafter periodically. Training was completed in January 2024.

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

21. Monitoring Arrangements

The DPL is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated as necessary. Otherwise, this policy will be reviewed **every 2 years** and shared with the full governing body.

22. Links with Other Policies

This data protection policy is linked to other policies including:

- Privacy Policy (no 7)
- Retention of Data Policy (56)
- AUP 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 alert the Head and the chair of governors
- The DPL 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 DPL will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPL 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 DPL 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 DPL must notify the ICO. The DPL 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 by the DPL on the School's central systems.

- Where the ICO must be notified, the DPL will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPL 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 DPL
 - 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 DPL 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 DPL expects to have further information. The DPL will submit the remaining information as soon as possible
- The DPL 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 DPL
 - 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, 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 by the DPL on the School's central systems.
- The DPL and Head 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

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 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 DPL as soon as they become aware of the error
 - If the sender is unavailable or cannot recall the email for any reason, the DPL will ask the ICT department to recall it
 - In any cases where the recall is unsuccessful, the DPL 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 DPL will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
 - The DPL 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
- Other types of breach that you might want to consider 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
- The school's cashless payment provider being hacked and parents' financial details stolen

Appendix 2 – DPIA Template

Name of System	Types of Information Stored, by whom and with whom	Main risk if data compromised (Data Impact)	Risk Mitigation (including score)
iSAMS	<ul style="list-style-type: none"> ▪ Pupil Data ▪ Pupil Attainment ▪ Home addresses ▪ Personal data ▪ Medical info ▪ Behaviour data ▪ Report card information 	<ul style="list-style-type: none"> ▪ Potentially a high risk if data is compromised. ▪ Potential to send wrong info to parents (pupils with same names). RW to help remind staff. ▪ Personal data breach is unlikely but possible – ICO report and specialist advice would be sought. 	<ul style="list-style-type: none"> ▪ Staff briefings on how to use and store information. ▪ Dep Hd and RW have regularly meetings with iSAMS to update on storage and use methods. ▪ INSET and Wed staff briefs. ▪ Cyber protection from MSP support via IT Manager.
CPOMS	<ul style="list-style-type: none"> ▪ Safeguarding and child protection info. ▪ Serious behaviour logged. ▪ Sensitive (very) information is retained. 	<ul style="list-style-type: none"> ▪ Safeguarding and child protection data is securely protected within the system. ▪ No external interfaces. ▪ Staff training at INSET. ▪ IT Manager sets configuration. ▪ Any breach would be very serious and reported. 	<ul style="list-style-type: none"> ▪ IT Manager sets configuration. ▪ Frequent staff training and checks on authority levels – done by SLT. ▪ Cyber protection from MSP support via IT Manager.
PASS Finance	<ul style="list-style-type: none"> ▪ Pupil Data ▪ Pupil Attainment ▪ Home addresses ▪ Staff information. ▪ Supplier details ▪ Fee payment details. ▪ Management account information/ ▪ Bank information / account information 	<ul style="list-style-type: none"> ▪ A real financial risk if any of PASS is released or hacked. ▪ Parent addresses and bank account information is stored and would be a major problem if released. ▪ Regular checks (Bursar and Dep Bursar) when checking and issuing invoices. 	<ul style="list-style-type: none"> ▪ IT Manager sets configuration. ▪ Frequent staff training from PASS account manager. ▪ Bursar and Hd Finance interrogate the system. ▪ Cyber protection from MSP support via IT Manager. ▪ Threats monitored by malware training.