



COOK LAWYERS
Employment Law and HR



St Paul's Catholic Primary School

'Together in Faith Working as One'

'We Shine!'

DATA PROTECTION POLICY

Policy created/updated **September 2026**

Due for review **September 2027**



Contents

1. Aims
2. Legislation and guidance
3. Definitions
4. The data controller
5. Roles and responsibilities
6. Data protection principles
7. Collecting personal data
8. Sharing personal data
9. Subject Access requests and rights of individuals
10. Parental requests to see the educational record
11. CCTV
12. Photographs and videos
13. Data protection by design and default
14. Data security and storage of records
15. Disposal of records
16. Personal data breaches
17. Training
18. Monitoring arrangements
19. Links with other policies

Appendix 1: Personal data breach procedure



Policy Cover Note

Title of the Policy	Data Protection
Statutory Requirement Y/N	Y
Decisions to be made / recommendation on options	
Name of the author	Cook Lawyers
Date written	July 2026
Date for review	July 2028
Summary of amendments / updates to policy	July 2026 update summary: policy updated to reflect the latest ICO and DfE guidance, including the DfE Data Protection in Schools guidance updated on 17 June 2026, the Data (Use and Access) Act changes now in force, ICO guidance on children's information and education information, and strengthened requirements for edtech, AI, CCTV, photos/videos, filtering and monitoring, retention, data sharing, subject access requests and breach response.



Data Protection Policy

1. Aims

The 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 at each of our academies.

2. Legislation and guidance

This policy meets the requirements of the UK GDPR, the Data Protection Act 2018 and the Data (Use and Access) Act 2025/2026 insofar as those provisions are in force. It is based on current guidance published by the Information Commissioner's Office (ICO), including guidance on UK GDPR, subject access requests, education information, children's information, data sharing, CCTV and video surveillance, personal data breaches, accountability and governance, and the ICO's June 2026 update on edtech compliance in schools.

This policy also reflects the Department for Education's Data Protection in Schools guidance, updated 17 June 2026, including the latest guidance on data protection responsibilities, records management, data retention, subject access requests, photos, videos, CCTV, generative AI, edtech, cyber security, filtering and monitoring, and safeguarding-related information sharing.

Where this policy refers to GDPR, it means the UK GDPR as retained and amended in UK law. The school will keep this policy under review as further ICO and DfE guidance is published following the implementation of the Data (Use and Access) Act.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individuals: • Name (including initials) • URN number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data, which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics



	• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything is 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 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 accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

The school process 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, will renew its registration annually or as otherwise legally required, and will ensure that its entry on the ICO register remains accurate and up to date.

5. Roles and responsibilities

This policy applies to **all staff** employed by our trust, 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 Governing Body has overall responsibility for ensuring that the school complies with all relevant data protection obligations.

5.2 Data protection officer

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

They will provide an annual report of their activities directly to the Governors and, where relevant, report to the board their advice and recommendations on school data protection issues.

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

Our DPO is Cook Lawyers - Mr John Cook and is contactable via john@cooklawyers.co.uk



5.3 Headteacher

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

5.4 All staff

Staff are responsible for:

Collecting, storing and processing any personal data in accordance with this policy

Informing the school of any changes to their personal data, such as a change of address

Contacting the DPO in the following circumstances:

- With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
- If they have any concerns, that this policy is not being followed
- If they are unsure whether or not they have a lawful basis to use personal data in a particular way
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties
- Before introducing or materially changing any edtech, AI-enabled tool, filtering or monitoring system, biometric system, CCTV system, online platform or app that processes personal data, particularly children's data
- Where they are considering sharing personal data for safeguarding, health, immunisation, law enforcement or public interest purposes and are unsure about the lawful basis or proportionality of the proposed sharing

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/carers 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.

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:

- There is an issue with a pupil or parent/carers 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 outside the UK, we will do so only where permitted by data protection law, including by using appropriate safeguards such as UK adequacy regulations, the UK International Data Transfer Agreement, the UK Addendum to the EU Standard Contractual Clauses or another lawful transfer mechanism, and by carrying out any required transfer risk assessment.

Where we use suppliers, processors, cloud services, edtech providers or AI-enabled systems, we will ensure that contracts clearly identify whether each party is acting as controller, joint controller or processor, include the mandatory processor terms where required, document data flows, restrict use of children's personal data to agreed purposes, and require appropriate security, retention, deletion and audit arrangements.

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 data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with



- How long will the data 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 do not need to use any particular form of words and may be made verbally or in writing, including by letter, email or through another communication channel. Staff must treat any request for a person's own personal data as a potential SAR and forward it immediately to the Headteacher and DPO.

- 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 Headteacher and DPO.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not to the child's parents or carers. A parent or carer may make a request on behalf of a child where they have parental responsibility, but the school will consider whether the child is competent to understand their rights and the implications of the request, whether the child has consented, and whether disclosure is in the child's best interests.

The ICO indicates that children under 12 are generally less likely to have sufficient maturity to understand their information rights, but this is not a fixed rule. The school will assess each request on a case-by-case basis, taking account of the pupil's age, maturity, capacity, any safeguarding concerns, the nature of the information requested and any views expressed by the pupil.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- 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.

If a SAR is received during a school closure period or school holiday, the one-month deadline still applies from receipt of the request unless the school is unable to verify identity or clarify the scope of the request, in which case the timescale may be paused in accordance with ICO guidance.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request, 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 DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see the educational record

For maintained schools in England, parents and those with parental responsibility have a separate right under the Education (Pupil Information) (England) Regulations 2005 to access their child's educational record within 15 school days of receipt of a written request. This right is separate from the UK GDPR right of access and does not apply in the same way to academies, free schools or independent schools. The school will consider which right applies before responding.



11. CCTV

We may use CCTV and other video surveillance systems in appropriate locations around the school site for specified purposes, such as security, safeguarding, health and safety, crime prevention and the protection of pupils, staff and visitors. The school will comply with ICO guidance on video surveillance and DfE guidance on taking and using photos, videos and CCTV in schools.

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

Any enquiries about the CCTV system should be directed to the school office.

Before installing or expanding CCTV or similar monitoring, the school will identify a lawful basis, consider whether a Data Protection Impact Assessment is required, ensure monitoring is necessary and proportionate, provide clear privacy information and signage, restrict access to recordings, apply appropriate retention periods and avoid using surveillance in areas where individuals have a high expectation of privacy unless there is an exceptional and lawful justification.

12. Photographs and videos

As part of day-to-day activities, the school may take photographs and record images of individuals.

Where the school takes photographs or videos for official school purposes, data protection law is likely to apply. We will tell pupils and parents/carers how images will be used, identify an appropriate lawful basis, obtain consent where consent is the appropriate basis, and ensure that any use of images is necessary, fair, transparent and proportionate.

Uses may include:

- Within school on noticeboards, newsletters, etc.
- Outside of school by external agencies such as the school photographer, local newspapers
- Online - school website or social media pages (e.g. Twitter)
- Sale of DVDs from Christmas Performances

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

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

Parents, carers and pupils will be reminded that data protection law does not usually apply to photographs or videos taken for purely personal or household use at school events, but school safeguarding, behaviour and online safety expectations may still apply. Where images are published publicly, the person publishing them may have data protection responsibilities.

13. Data protection by design and default

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

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law



- Completing privacy impact assessments where the school processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure the schools are compliant
- Maintaining records of our processing activities, including:
 - For the benefit of data subjects, making available the name and contact details of the school and DPO and all the information we are required to share about how we use and process their personal data (via The School Privacy Notices)
 - For all personal data that is held, 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 the trust is storing the data, retention periods and how we are keeping the data secure
 - Completing and documenting Data Protection Impact Assessments before high-risk processing, including new or changed use of edtech, generative AI, biometric systems, CCTV or monitoring, large-scale processing, profiling, automated decision-making, or processing involving children's information where there may be a high risk to rights and freedoms
 - Maintaining appropriate records of processing activities, privacy notices, lawful basis assessments, special category and criminal offence data conditions, data sharing decisions, supplier due diligence, contracts, retention decisions, breaches, rights requests and staff training

14. Data security and storage of records

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

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Strong, unique passwords, multi-factor authentication where available, role-based access controls and timely removal of access for leavers or role changes are used to protect school systems, accounts and devices. Staff and pupils must not share passwords and must follow the school's cyber security and acceptable use requirements.



- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our online safety policy/acceptable use policy)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)
- Filtering and monitoring systems used for safeguarding and online safety will be configured, reviewed and managed in a way that is lawful, proportionate, transparent and secure, with access to monitoring information restricted to staff who need it for safeguarding, pastoral, technical or legal reasons.

15. Disposal of records

Personal data that is no longer needed will be disposed of securely. The school will maintain and review a data retention schedule, carry out periodic personal data audits, and check at least annually whether the personal data it holds remains accurate, necessary and proportionate for the purposes for which it is retained.

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/trust's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Where records need to be retained for longer because of safeguarding, legal proceedings, an information rights request, an investigation, a legal hold or another lawful reason, the school will document the reason and set a revised review or destruction date. Personal data must not be retained indefinitely without a documented lawful reason.

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.

If a personal data breach is likely to result in a risk to individuals' rights and freedoms, we will report it to the ICO without undue delay and, where feasible, within 72 hours of becoming aware of it. If the risk to individuals is high, we will also inform affected individuals without undue delay unless an exemption or lawful reason not to do so applies. 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.

Training will include practical guidance on recognising SARs and other rights requests, reporting data breaches promptly, handling children's information, using edtech and AI safely, sharing information for safeguarding, applying retention periods, and following cyber security, filtering and monitoring procedures.

18. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed **every 2 years** and shared with school personnel and governors.

19. Links with other school policies

This data protection policy is linked to our:

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

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

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored in the school office
- 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 description of the nature of the personal data breach including, where possible:
 - The categories and approximate number of individuals concerned
 - The categories and approximate number of personal data records concerned
 - The name and contact details of the DPO
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned



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

Records of all breaches will be stored by the school and the DPO.

The DPO and the school will review what happened and how it can stop it 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 a special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the 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
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request



- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.