

Data protection policy

St Peter & St Paul CE Primary



Approved by:	Governors	Date	September 2026
Last reviewed on:	September 2026		
Next review due by:	Autumn 2027		

Contents

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

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the [General Data Protection Regulation \(GDPR\)](#) and the 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 UK GDPR and the Data Protection Act 2018. It also incorporates provisions from the Data (Use and Access) Act 2025 regarding modernised data access procedures and complaint handling.

It is based on guidance published by the Information Commissioner's Office (ICO), including the statutory guidance for Subject Access Requests (SARs) and the ICO guidance on video surveillance (CCTV) and emerging biometric systems.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents of pupils at maintained schools the right of access to their child's educational record. It also aligns with the Department for Education's (DfE) statutory 'Data protection in schools' guidance including the latest DfE rules on digital technology, AI usage, and online safety filtering.

3. Definitions

Term	Definition
Personal data	<p>Any information relating to an identified, or identifiable, living individual.</p> <p>For our school, this includes names, initials, identification numbers, online identifiers (like usernames, IP addresses, and device IDs), and location data. It can also include physical, mental, economic, or social details.</p>
Special categories of personal data	<p>Personal data that is highly sensitive and needs extra protection. This includes information about:</p> <ul style="list-style-type: none">• Racial or ethnic origin• Political opinions• Religious or philosophical beliefs• Trade union membership• Genetics and biometric data (e.g.,

	fingerprints or facial recognition for identification) • Physical or mental health • Sex life or sexual orientation
Processing	Anything done to personal data. This includes collecting, recording, organising, storing, changing, retrieving, using, sharing, erasing, or destroying it. Processing can be digital or on paper.
Data subject	The living individual whose personal data is held or processed (such as a pupil, parent, staff member, or governor).
Data controller	The organisation that decides how and why personal data is used. For our school, the legal Data Controller is the Governing Body.
Data processor	A person or external business (other than a school employee) that handles personal data on behalf of the data controller. This includes our online learning apps, catering systems, and IT support providers.
Personal data breach	A security incident where personal data is accidentally or unlawfully lost, destroyed, changed, shared without permission, or accessed by the wrong person.

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 Governing Body of St Peter & St Paul CE Primary School is the legal Data Controller and holds ultimate responsibility for compliance with data protection legislation.

The school is registered with the Information Commissioner's Office (ICO) as a data controller under registration number ZA233687. This registration is renewed annually by the school business manager, and the required data protection fee is paid.

5. Roles and responsibilities

This policy applies to all staff employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governing board

The governing board has overall legal responsibility for ensuring that our school complies with all relevant data protection obligations as the Data Controller.

5.2 Data protection officer (DPO)

The DPO is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and providing independent advice on Data Protection Impact Assessments (DPIAs) and data breaches.

The DPO acts as the independent point of contact for individuals whose data the school processes, handles escalated data protection complaints under the Data (Use and Access) Act 2025, and acts as the liaison for the ICO. They provide an annual report of their compliance findings directly to the governing board.

Our appointed DPO is the School Business Manager and is contactable via the school phone number and admin email address. The School Business Manager also acts as the internal Data Protection Lead to support day-to-day administration.

5.3 Headteacher

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

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 United Kingdom.
 - ☐ If there has been a data breach.
 - ☐ Whenever they are engaging in a new activity that may affect the privacy rights of individuals, including the use of Artificial Intelligence (AI) tools or biometric systems
 - ☐ If they need help with any contracts or sharing personal data with third parties.
 - ☐ If they receive any formal data protection complaints or Subject Access Requests (SARs) from individuals.

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
 - ☐ Handled in a way that allows the school to take responsibility for compliance and demonstrate how we meet these rules (Accountability).

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 (except where the school is acting as a public authority carrying out its official tasks), 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). Our use of online services will always align with the ICO's Children's Code.

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 school's record retention schedule and records management policy.

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so under specific circumstances such as staff safety risks, liaising with other agencies with consent, or when required by law enforcement, safeguarding obligations, or emergency response situations.

For suppliers and contractors (including IT companies and educational software providers), we ensure compliance by appointing verified providers, requiring prior DPO approval before using third-party apps, establishing data-sharing agreements, and limiting shared data to necessary services. International transfers outside the United Kingdom (UK) will use appropriate safeguards like the UK International Data Transfer Agreement or UK Addendum 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' (SAR) to gain access to personal information that the school holds about them. This includes confirmation of processing, copies of their data, processing purposes, categories of data concerned, data recipients, retention periods, data sources, and details of any automated decision-making.

SARs can be made in writing. While the school may ask for specific details (such as the individual's name, contact info, and clear details of the information requested) to help locate the data, a request cannot be refused if the individual chooses not to provide these format details. The school will verify the identity of the requester before disclosing any data.

If staff receive a subject access request they must immediately forward it to the DPO. In line with the Data (Use and Access) Act 2025, the school will respond within one calendar month and will conduct searches that are reasonable and proportionate to locate the requested data. The school reserves the right to refuse or charge a fee for requests that are deemed vexatious or excessive.

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 school must verify that the requester holds legal parental responsibility. The child must also either be unable

to understand their rights and the implications of a subject access request, or have given their explicit consent.

Children below the age of 12 are generally presumed not to be mature enough to understand their rights and the implications of a subject access request. Therefore, subject access requests from parents or carers of pupils under 12 may typically be granted without the express permission of the pupil, provided disclosure is in the child's best interests.

This is not a fixed rule. A pupil's ability to understand their rights will always be judged on a case-by-case basis, taking into account their maturity, understanding, and any specific safeguarding vulnerabilities.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide two forms of identification to verify their identity. The statutory response timeframe will only begin once identity is confirmed.
- May contact the individual via phone to confirm the request was made.
- Will respond without delay and within one calendar month of receipt of the valid request.
- May temporarily pause the one-month deadline ('stop the clock') if we reasonably require clarification from the requester regarding the scope of the data requested. The clock will resume the day after the necessary clarification is received.
- Will provide the information free of charge and limit our searches to what is reasonable and proportionate to locate the requested data.
- May tell the individual we will comply within three months of receipt of the request where a request is complex or numerous. We will inform the individual of this within the first 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 given to a court in proceedings concerning the child.
- Is protected by legal professional privilege (such as confidential correspondence between the school and our solicitors).

If a request is manifestly unfounded or excessive, we may refuse to act on it or charge a reasonable fee to cover administrative costs. A request may be deemed manifestly unfounded or excessive if it is repetitive, asks for further copies of the same information, or is explicitly intended to cause disruption.

When we refuse a request, we will tell the individual why. We will also inform them of their right to log a formal dispute through the school's internal data protection complaints procedure, or escalate the matter to the ICO or the courts if they remain unsatisfied with our internal response.

9.4 Other data protection rights of the individual

In addition to subject access and collection notices, individuals have the right to withdraw consent, rectify/erase/restrict/object to processing, prevent direct marketing, challenge public interest processing, and request data portability. Updates include transferring data outside of

the United Kingdom (UK), requesting human review of automated decisions, and utilizing an internal complaint procedure (acknowledged within 30 days) before escalating to the ICO.

Requests must be submitted or forwarded immediately to the DPO.

10. Parental requests to see the educational record

In accordance with the Education (Pupil Information) (England) Regulations 2005, parents or those with parental responsibility at maintained schools have a legal right to view their child's educational record free of charge. This must be made available within 15 school days of receiving a written request. If a parent requests a copy of the record, the school may charge a reasonable fee that does not exceed the actual cost of supply. The school reserves the right to withhold information if disclosure would likely cause serious harm to the physical or mental health of the pupil or another individual

11. CCTV and Video Surveillance

We use a Closed-Circuit Television (CCTV) system across various external and internal locations on the school site. The system is operated purely to maintain a safe environment, deter violent behaviour, and protect school buildings and assets from vandalism or crime

Our usage of video surveillance adheres strictly to data protection laws and the ICO Video Surveillance Guidance.

To ensure complete compliance, the school enforces the following rules:

- **Transparency:** While individual consent is not required to record for security purposes, clear and visible warning signs are placed at main entrances and within recording zones.
- **Storage and Retention:** Recorded footage is stored digitally in a secure, encrypted environment. Data is retained for no longer than 30 days, after which it is automatically overwritten, unless required as part of an active criminal investigation or legal proceeding.
- **Restricted Access:** Access to view live or historical footage is password-protected and strictly limited to authorized personnel (the Headteacher, Admin Officer, Pastoral team and Senior Leadership Team). Staff misuse of surveillance data will trigger immediate disciplinary actions.

Any data protection queries regarding the surveillance system should be directed to the Data Protection Officer (DPO). Operational enquiries can be raised with the School Business Manager or Headteacher.

12. Photographs and videos

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

We will obtain separate, granular written consent from parents/carers for photographs and videos to be taken of their child. We will clearly explain how the media will be used, allowing parents to opt-in or opt-out of specific categories.

Uses are strictly managed under separate consent channels, including:

- **Internal School Use:** Displays on notice boards, internal learning platforms, and printed school newsletters or magazines.

- External Agencies: The official school photographer, local journalism, or trusted educational campaigns.
- Public Online Channels: The official school website or verified school social media accounts.

Device Security and Storage: All images must be captured using school-owned devices (such as school iPads or cameras) and stored securely on the school's authorized, encrypted cloud network. Staff are strictly prohibited from using personal mobile phones or personal devices to photograph or record pupils.

Withdrawal of Consent: Consent can be refused or withdrawn at any time. If consent is withdrawn, the school will immediately remove the digital image from our website/social media and stop any future distribution. Requesters should note that the school cannot destroy or recall physical materials (such as printed brochures or past newspapers) that were already published before consent was withdrawn.

Parental Photography at Events: Parents and carers **are not** permitted to take photographs and videos at open school events (such as sports days and plays) for their own personal, domestic use.

See our child protection and safeguarding policy, and our digital media consent form, for more information on our use of photographs and videos.

13. Data protection by design and default

We will put technical and organizational measures in place to demonstrate that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified Data Protection Officer (DPO), 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, in line with the data protection principles set out in relevant data protection law (see section 6).
- Completing formal Data Protection Impact Assessments (DPIAs) whenever processing presents a high risk to the rights and freedoms of individuals, and automatically prior to introducing any new technologies, including Artificial Intelligence (AI) tools, biometrics, or third-party cloud applications. The DPO will advise on and oversee this process.
- Integrating data protection into the procurement process, ensuring all third-party software and systems undergo thorough data protection vetting before adoption.
- Integrating data protection into internal documents, including this policy, related policies, and privacy notices.
- Regularly training all members of staff on data protection law, this policy, and related procedures, while maintaining an active, verifiable record of attendance.
- Regularly conducting reviews and audits to test our privacy measures and ensure ongoing compliance.
- Maintaining a comprehensive, internal Record of Processing Activities (ROPA). This ROPA will document the types of data held, data subjects, processing purposes, third-party recipients, international transfer safeguards, retention periods, and specific technical security measures used to keep the data secure.
- Making the name and contact details of our school and DPO easily accessible via our privacy notices.

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:

- **Physical Security:** Paper-based records and portable electronic devices (such as school laptops and encrypted drives) that contain personal data must be kept locked away when not in use. Papers containing confidential personal data must never be left unattended on desks, staffroom tables, or anywhere with general access.
- **Off-site Data Control:** Where physical personal information must be taken off-site, explicit authorization must be obtained from a line manager, and a log maintained by the school office.
- **Password and Access Control:** Access to school networks and devices requires strong passwords and staff will be forced to change passwords at regular intervals.
- **Multi-Factor Authentication (MFA):** MFA is mandatory for all staff accessing school systems, cloud environments (such as emails), and management information systems (MIS) remotely.
- **Removable Media:** The use of USB sticks and unencrypted removable hard drives to store personal data is strictly prohibited. Staff must use the school's approved, secure cloud storage network.
- **Personal Devices (Bring Your Own Device - BYOD):** Staff, pupils, and governors may use personal devices to view school systems via secure, authenticated web portals. However, downloading or storing local copies of school personal data onto personal devices is strictly prohibited.
- **Encryption:** Encryption software is applied to all school-owned portable devices.
- **Third-Party Security:** Where we share personal data with a third party, we carry out strict due diligence to ensure it is stored securely and adequately protected (see section 8).

15. Disposal of records

Personal data that is no longer needed, or that has become inaccurate or out of date and cannot be rectified, will be disposed of securely in accordance with the school's record retention schedule (based on the IRMS Information Management Toolkit for Schools).

- **Paper-Based Records:** Confidential paper records will be shredded on-site using a cross-cut shredder or collected by an authorized confidential waste partner.
- **Electronic Files:** Digital data will not simply be deleted; it will be permanently and securely purged from active systems, servers, and cloud recycling bins.
- **Hardware and Devices:** Old computers, hard drives, mobile devices, and storage media will be securely degaussed, wiped, or physically destroyed by certified specialists in compliance with data protection laws and WEEE (Waste Electrical and Electronic Equipment) regulations.
- **Third-Party Disposal:** Where a third party is used to safely dispose of records or hardware on the school's behalf, the school will conduct strict due diligence. The school will require and retain formal written Certificates of Destruction from the supplier to maintain a clear audit trail.

16. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the event of a suspected data breach, we will follow the step-by-step procedure set out in Appendix 1.

- **ICO Notification:** The school will report any personal data breach to the ICO without undue delay and, where feasible, within 72 hours of becoming aware of it. A report is legally required unless the breach is unlikely to result in a risk to the rights and freedoms of individuals.
- **Data Subject Notification:** If a breach is deemed to result in a high risk to the rights and freedoms of individuals (such as severe safeguarding leaks or identity theft risks), the school will notify the affected individuals directly and without undue delay.
- **Internal Recording:** The DPO will maintain a central, internal Data Breach Register. Every suspected or confirmed breach, including the facts, its effects, and the remedial actions taken, will be recorded in this register, regardless of whether it meets the threshold to be reported to the ICO.

School-context breaches include, but are not limited to: publishing non-anonymised pupil premium exam results online, disclosing safeguarding information to unauthorised persons, or the theft of an unencrypted school device containing personal data.

17. Training

All staff, including temporary and agency workers, are provided with mandatory data protection training.

To ensure ongoing compliance and maintain operational awareness:

- **Annual Refresher Training:** All staff must complete data protection refresher training at least once every academic year.
- **Targeted Training:** Staff in high-risk data roles—including the Designated Safeguarding Lead (DSL), SENCo, School Business Manager, and administrative teams—will receive additional specialized training tailored to their specific operational duties.
- **Governance Training:** Members of the Governing Board (or Board of Trustees) will receive regular data protection training to ensure they understand their legal liabilities and oversight responsibilities.
- **Auditable Records:** The school will maintain a centralized training log documenting completion dates, attendance, and training modules. Staff who fail to complete mandatory sessions will be flagged for immediate follow-up.
- **Ad-Hoc Updates:** Data protection briefings will form part of continuing professional development (CPD) whenever there are sudden changes to national legislation, official guidance, or internal school processes.

18. Monitoring arrangements

The Data Protection Officer (DPO) is responsible for monitoring, reviewing, and updating this policy to ensure it remains compliant with all relevant legislation and statutory guidance.

This policy will be reviewed annually to reflect evolving cybersecurity risks, ICO updates, and legislative changes, including the Data (Use and Access) Act 2025.

Following its annual review, the updated policy will be presented to the full governing board [or Board of Trustees] for formal approval and sign-off at the start of each academic year.

19. Links with other policies

This data protection policy is linked to our:

Information Security Policy

Records Management Policy

Privacy Notices

Appendix 1: Personal data breach procedure

This procedure is based on statutory guidance on personal data breaches produced by the ICO and complies with the reporting frameworks under UK data protection law.

1. Immediate Action and Reporting

On finding or causing a breach, or a potential breach, the staff member or data processor must take the following immediate steps:

- Immediate Containment: Take any safe, immediate action possible to stop the breach from spreading (e.g., close an open window, disconnect a compromised computer from the network, or ask an accidental email recipient to delete the message). Staff must not attempt to alter or delete system logs.
- Immediate Notification: Notify the Data Protection Officer (DPO) immediately, and within a maximum of 24 hours of discovery, by emailing [Insert DPO Email/System Link].
- Provide Critical Initial Details: The notification to the DPO should, wherever possible, include:
 - A brief description of what happened.
 - The date and time the incident occurred and when it was discovered.
 - The categories and approximate number of data subjects affected (e.g., 30 Year 9 pupils, 2 staff members).
 - The types of personal data involved (e.g., names, addresses, safeguarding markers, health records).

2. DPO Investigation and Risk Assessment

Upon receiving the report, the DPO will immediately instigate an investigation to determine whether a breach has occurred and evaluate its severity. The DPO will consider whether personal data has been accidentally or unlawfully:

- Lost or stolen.
- Destroyed or altered without authorization.
- Disclosed, made available, or accessed by unauthorized individuals.

Risk Assessment: The DPO will conduct a formal risk assessment to determine the potential impact on the rights and freedoms of the affected individuals. This assessment will categorize the incident as:

- Low Risk: Unlikely to cause harm (no external notification required; logged internally).
- Medium/High Risk: Likely to result in a risk to individuals (triggers mandatory ICO notification within 72 hours).
- Very High Risk: Likely to cause severe harm or distress (triggers mandatory notification to both the ICO and the affected individuals without undue delay).

3. Containment, Evaluation, and Escalation

- Immediate Containment: The DPO, assisted by relevant staff members, network administrators, or data processors, will make all reasonable efforts to immediately contain the breach and minimise its impact. (*Specific containment actions for different data types are detailed at the end of this procedure*).
- Leadership Notification: Simultaneously with containment, the DPO will alert the Headteacher and the Chair of Governors to ensure executive oversight and mobilize any necessary emergency resources.
- Consequence Assessment: The DPO will formally assess the potential consequences of the breach, evaluating both the severity of the impact and the likelihood of it occurring.

- **ICO Reporting Determination:** The DPO will determine on a case-by-case basis whether the breach must be reported to the ICO. This assessment and any required notification must be completed within 72 hours of the school becoming aware of the incident.
- **Evaluating Harm:** A report to the ICO is legally mandatory unless the breach is unlikely to result in a risk to individuals' rights and freedoms. To decide, the DPO will assess if the breach could cause physical, material, or non-material damage (such as emotional distress), including through:
 - Loss of control over personal or sensitive data.
 - Discrimination or damage to reputation.
 - Identity theft, fraud, or financial loss.
 - Unauthorised reversal of pseudonymisation (re-identifying coded data).
 - Loss of confidentiality or any other significant economic or social disadvantage.
- **Documentation of Low-Risk Breaches:** If the DPO concludes that the breach is unlikely to pose a risk and does not require an ICO report, the DPO will formally document the justification and decision within the school's internal Data Breach Register to ensure compliance with accountability standards.

4. Documenting and Reporting the Breach

- **Central Documentation:** The DPO will formally document every breach decision (whether reported to the ICO or not) in the school's central Data Breach Register. These records will be stored securely on the school's restricted administrative network to maintain a permanent, legally robust audit trail.
- **ICO Notification Content:** Where an ICO notification is required, the DPO will submit the report via the official ICO portal within 72 hours. The report will include:
 - A description of the nature of the breach, including the categories and approximate number of individuals and data records concerned.
 - The name and contact details of the DPO.
 - A description of the likely consequences of the breach.
 - A clear summary of the mitigation measures already taken, or planned, to address the breach and protect affected individuals.
- **Phased Reporting:** If full details are not available within 72 hours, the DPO will submit a phased report containing all currently available facts. The initial submission will explain the reasons for the delay and specify when the remaining information will be provided. The outstanding data will then be submitted without undue delay as the investigation progresses.
- **Notifying Affected Individuals:** If the breach is determined to pose a high risk to the rights and freedoms of individuals, the DPO will notify the affected parties directly, in clear and plain language, without undue delay. This notification will explicitly state:
 - The nature of the breach and the contact details of the DPO.
 - The likely consequences of the data leak.
 - The specific actions the school is taking to protect them, alongside practical steps they can take themselves (e.g., changing passwords or monitoring bank accounts).
 - Details on how they can submit a formal dispute through the school's internal data protection complaints procedure if they are dissatisfied with the school's response.

5. Mitigation, Governance, and Review

- **Third-Party Assistance:** The DPO will promptly notify and collaborate with relevant external bodies that can help mitigate harm to individuals. This includes the police, local safeguarding partners, cyber security experts, insurers, or financial institutions where relevant.
- **Centralized Accountability Log:** Every single suspected or confirmed breach will be recorded in the school's central Data Breach Register, regardless of whether it is reported

to the ICO. Each entry will document the timeline, root cause, specific data sets affected, operational impacts, and all containment actions taken.

- **Secure Data Storage:** The Data Breach Register and all supporting evidence will be stored permanently on the school's secure, restricted administrative network, ensuring an immutable audit trail for future regulatory review.
- **Post-Incident Review:** As soon as reasonably possible following containment, the DPO, Headteacher, and relevant operational leads will meet to conduct a root-cause analysis.
- **Action Plan and Reporting:** This review will produce a formal action plan to update security protocols, modify internal processes, or deliver targeted staff training. A summary of the breach, the lessons learned, and any updates to the school's risk register will be formally reported to the Governing Board at their next scheduled meeting.