



Priory Junior School

Data Protection Policy

2026/27

Policy owner	Governing Body / Headteacher
Headteacher	Mr Jack Cross
Data Protection Officer (DPO)	Samantha Ford
DPO contact	0115 952 6100 office@priory-jun.notts.sch.uk
Last reviewed	August 2026
Governing Body approval	To be confirmed
Review date	August 2027, or immediately if the school's legal status/data controller changes
School	Priory Junior School, Priory Road, Gedling, Nottingham, NG4 3LE

We LEARN with PRIDE

Peace - Respect - Independence - Determination - Equality

Contents

1. Aims and scope
2. Legislation and guidance
3. Definitions
4. Data controller and governance
5. Roles and responsibilities
6. Data protection principles
7. Lawful, fair and transparent processing
8. Privacy information and records of processing
9. Sharing personal data and safeguarding information
10. Individual rights and subject access requests
11. Parental access to educational records
12. Biometric recognition systems
13. CCTV
14. Photographs and videos
15. Artificial intelligence, automated decision-making and EdTech
16. Filtering and monitoring
17. Data protection by design and default
18. Data security and storage
19. Retention and disposal
20. Personal data breaches and cyber incidents
21. Data protection complaints
22. Training, monitoring and review
23. Linked policies and documents
- Appendix 1: Personal data breach procedure
- Appendix 2: Staff quick guide - protect personal data

1. Aims and scope

Priory Junior School is committed to protecting the personal information of pupils, parents and carers, staff, governors, volunteers, visitors and other individuals. We will collect, use, store, share and dispose of personal data lawfully, fairly, transparently and securely, and we will be able to demonstrate our compliance.

This policy applies to all personal data processed by or on behalf of the school, whether held electronically, in cloud services, within school systems such as the MIS or CPOMS, in photographs or recordings, or in paper records. It applies to all staff, governors, volunteers, contractors and third parties acting on the school's behalf.

Safeguarding comes first: Data protection law does not prevent the lawful sharing of information needed to safeguard a child or another person. Staff must follow the Child Protection Policy and report safeguarding concerns without delay. A concern about data protection must never be allowed to delay an urgent safeguarding response.

2. Legislation and guidance

This policy is based on the current data protection framework and relevant education guidance, including:

- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018;
- Data (Use and Access) Act 2025 (DUAA), which amends and builds on the UK GDPR and Data Protection Act 2018;
- Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020 and the Privacy and Electronic Communications Regulations where relevant;
- Education (Pupil Information) (England) Regulations 2005, while Priory Junior School remains a maintained school;
- Protection of Freedoms Act 2012 in relation to any future automated biometric recognition system;

- Information Commissioner’s Office (ICO) guidance, including guidance on children’s information, individual rights, data sharing, security, surveillance and data breaches;
- Department for Education (DfE) guidance: Data protection in schools, including the Data Use and Access Act 2025, generative AI, EdTech procurement, photographs/videos/CCTV, cyber security and filtering and monitoring;
- DfE Meeting digital and technology standards in schools and colleges, including the Cyber security and Filtering and monitoring core standards; and
- Keeping Children Safe in Education 2026 and Working Together to Safeguard Children 2026 where personal data is processed for safeguarding purposes.

Where legislation or statutory guidance changes, the school will apply the current legal requirements and review this policy as necessary.

3. Definitions

Term	Meaning
Personal data	Information relating to an identified or identifiable living individual, directly or indirectly. This includes names, identifiers, location data, online identifiers and information about a person’s physical, mental, economic, cultural or social identity.
Special category data	More sensitive personal data requiring additional protection, including racial or ethnic origin, political opinions, religious/philosophical beliefs, trade union membership, genetic and biometric data used for identification, health data, and information about sex life or sexual orientation.
Criminal offence data	Personal data relating to criminal convictions, offences, allegations or related security measures. Additional legal conditions apply.
Processing	Any operation performed on personal data, including collecting, recording, organising, storing, viewing, using, sharing, transmitting, altering, anonymising, erasing or destroying.
Data subject	The identified or identifiable living individual to whom personal data relates.
Data controller	The organisation that determines why and how personal data is processed.
Data processor	A separate person or organisation that processes personal data on the controller’s documented instructions.
Personal data breach	A security breach leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
DPIA	A Data Protection Impact Assessment used to identify and reduce privacy risks before high-risk processing or significant new technology is introduced.
Pseudonymisation	Processing personal data so it cannot be attributed to a specific person without additional information kept separately and securely.

4. Data controller and governance

At the date this policy is adopted, Priory Junior School is a maintained community school and acts as a data controller for most personal data that it determines how and why to process. The school is registered with the ICO and pays the applicable data protection fee as legally required.

The Governing Body has overall responsibility for ensuring that the school complies with data protection law. The Headteacher acts as the representative of the data controller for day-to-day management, supported by the DPO and relevant staff.

5. Roles and responsibilities

5.1 Governing Body

- has overall accountability for data protection compliance and provides appropriate oversight;
- ensures an appropriately independent and suitably qualified DPO is appointed and resourced;
- ensures risks arising from new technology, cyber security and significant data processing are understood and managed;
- receives appropriate assurance, including DPO reporting, audit information and significant breach information; and
- ensures this policy and associated privacy notices and procedures are reviewed regularly.

5.2 Data Protection Officer (DPO)

The school’s DPO is Samantha Ford. The DPO can be contacted via 0115 952 6100 or office@priory-jun.notts.sch.uk. Correspondence should be marked for the attention of the Data Protection Officer.

- oversees implementation of this policy and monitors compliance;
- advises on data protection law, lawful bases, individual rights, DPIAs, contracts, sharing and security;
- is the first point of contact for the ICO and for data subjects on data protection matters;
- provides advice independently and reports concerns to the Governing Body as appropriate;
- maintains appropriate records of breaches, complaints, DPIAs and processing activities; and
- provides or coordinates data protection training and awareness.

The school will ensure that the DPO is able to perform the role independently and is not instructed on the conclusions they should reach. Any potential conflict of interest will be identified and managed.

5.3 Headteacher and senior leaders

- ensure staff follow this policy and that data protection is integrated into school systems and decisions;
- consult the DPO before high-risk processing, major changes in systems, new AI/EdTech, monitoring or significant data-sharing arrangements;
- ensure suspected breaches and cyber incidents are escalated immediately; and
- ensure suppliers, contractors, volunteers and visitors are given appropriate access only to the information needed for their role.

5.4 All staff, governors and volunteers

Everyone who handles personal data for the school is responsible for protecting it. They must:

- only access, use or share personal data when there is a clear work-related need and appropriate authority;
- keep information accurate, relevant, secure and confidential;
- follow school procedures for email, passwords, devices, cloud storage, paper records, photographs and communication;
- immediately forward any request to exercise data protection rights to the DPO; and
- immediately report any actual or suspected personal data breach, loss, misdirection, unauthorised disclosure, phishing compromise or inappropriate use of personal data in an AI or other online tool.

6. Data protection principles

Priory Junior School will apply the data protection principles. Personal data will be:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes and not used incompatibly with those purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- kept for no longer than necessary;
- processed securely to protect confidentiality, integrity and availability;
- transferred outside the UK only where lawful safeguards apply; and
- handled in a way that respects the rights of data subjects.

The school is accountable for these principles and must be able to demonstrate compliance through policies, privacy notices, contracts, records, DPIAs, security controls, training and review.

7. Lawful, fair and transparent processing

7.1 Lawful bases for personal data

The school will identify and document an appropriate lawful basis for each processing activity. Depending on the activity, the lawful basis may be:

- contract - processing necessary for a contract or steps requested before entering a contract;
- legal obligation - processing necessary to comply with the law;
- vital interests - processing necessary to protect someone's life;
- public task / official authority - processing necessary for the school's functions laid down by law;
- consent - freely given, specific, informed and unambiguous consent that can be withdrawn;
- legitimate interests - only where legally available and appropriate; public authorities cannot rely on ordinary legitimate interests for processing carried out in performance of their public tasks; and
- recognised legitimate interests - where processing is necessary for a purpose expressly recognised in the UK GDPR as amended by the DUA. The DPO will advise before this basis is relied upon.

Consent will not be used simply because it appears convenient. Where the school has a legal obligation or public task, that is usually more appropriate. Withdrawal of consent does not affect processing that has another lawful basis.

7.2 Special category and criminal offence data

Where the school processes special category data, it will have both an Article 6 lawful basis and an additional condition under Article 9 and the Data Protection Act 2018. Where required, the school will maintain an Appropriate Policy Document. Criminal offence data will only be processed where a lawful basis and a specific legal condition apply.

Examples of special category processing in school include medical conditions, allergies, SEND-related health information, safeguarding, equality monitoring, occupational health and information about religious beliefs where relevant to school provision.

7.3 Children's personal data

Children require particular protection because they may be less aware of the risks, consequences and their rights. Priory will use clear, age-appropriate explanations where pupils are directly involved in data processing, apply data minimisation, and take account of the ICO Children's Code where an online service is likely to be accessed by children.

8. Privacy information and records of processing

When personal data is collected, the school will provide the information required by law through appropriate privacy notices. Privacy information will explain, in clear language, what data is used, why, the lawful basis, who it may be shared with, how long it is kept, relevant rights and how to contact the DPO.

The school will maintain appropriate records of processing activities, including the categories of personal data and data subjects, purposes, lawful bases, recipients, international transfers, retention periods and key security measures. Privacy notices will be reviewed when systems, suppliers or purposes change.

9. Sharing personal data and safeguarding information

Personal data will only be shared when there is a lawful basis and the sharing is necessary, proportionate and secure. Before routine or systematic sharing with a third party, the school will carry out appropriate due diligence and put written data-processing or data-sharing arrangements in place where required.

- Only the minimum information needed for the purpose will be shared.
- Staff must check the identity and authority of the recipient before disclosure.
- Secure methods will be used for sensitive information, and email recipients will be checked carefully before sending.
- Processors will only be appointed where they provide sufficient guarantees of compliance, security and confidentiality, and contracts will include the required data protection terms.
- International transfers will only take place where UK data protection law permits them and appropriate safeguards are in place.

9.1 Safeguarding and child protection

Information may be shared without consent where this is necessary to safeguard a child or another person, comply with a legal obligation, perform a public task, protect vital interests or where another lawful basis applies. Staff should be open with families about information sharing where it is safe and appropriate to do so, but consent must not be sought where doing so could place a child or another person at increased risk or prejudice a safeguarding response.

Safeguarding information must be shared on a need-to-know basis, recorded accurately and handled in accordance with the Child Protection Policy, KCSIE and local safeguarding procedures.

10. Individual rights and subject access requests

Individuals have rights in relation to their personal data. Depending on the circumstances, these include the rights to be informed; access; rectification; erasure; restriction; objection; data portability; withdrawal of consent; and safeguards in relation to significant solely automated decisions. These rights are not absolute and may be limited by law.

10.1 Recognising a subject access request (SAR)

A SAR is a request by an individual for access to their own personal data. A request does not have to use the words "subject access request", cite legislation or be made on a particular form. It can be made verbally or in writing. Staff who receive a possible SAR must forward it to the DPO immediately and must not attempt to answer it informally.

10.2 Children and SARs

Personal data about a child belongs to the child. A parent or carer may exercise the child's right of access where the child is not competent to understand and exercise the right themselves, or where the child has authorised the parent/carers. In a primary school, children below 12 will often not have sufficient understanding, but this is not an automatic rule and competence will be considered case by case.

10.3 Responding to SARs

- The school will respond without undue delay and normally within one calendar month.
- Where identity or authority is genuinely uncertain, the school may request reasonable and proportionate evidence. The response period will begin when necessary identity/authority information is received.
- Where a request is complex or the individual has made a number of requests, the response period may be extended by up to a further two months. The individual will be told within the first month and given reasons.
- Where clarification of the information requested is reasonably required to provide an effective response, the school may ask for clarification. The response clock pauses from the day clarification is requested and resumes the day after it is received.
- The school is required to make reasonable and proportionate searches for relevant information.

- SARs are normally free of charge. A reasonable fee may be charged where permitted by law, including for manifestly unfounded or excessive requests or further copies.
- Information relating to other people will be redacted or withheld where disclosure would be unlawful or unreasonable, and statutory exemptions will be applied where relevant.

If the school refuses to act on all or part of a request, it will explain the reasons and inform the individual of their right to complain to the ICO or seek a judicial remedy.

11. Parental access to educational records

While Priory Junior School remains a maintained school, 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. This is different from a SAR.

- A written request to see the educational record will be dealt with within 15 school days.
- Access to the record is free. If a copy is requested, the school may charge no more than the cost of supplying it.
- The right applies while the pupil is under 18 and is subject to statutory restrictions, including where disclosure could cause serious harm or where specified information is exempt.

This section must be reviewed if the school converts to academy status, because the statutory educational-record access regime differs for academies. Data protection rights, including SAR rights, continue regardless of school status.

12. Biometric recognition systems

This policy does not authorise the introduction of an automated biometric recognition system for pupils. If the school proposes to use fingerprints, facial recognition or other biometric data for automated recognition, it will first obtain DPO advice, complete a DPIA, obtain the required approvals, notify parents/carers, comply with the Protection of Freedoms Act 2012 and provide a suitable non-biometric alternative. A child's refusal to participate will be respected regardless of parental consent.

13. CCTV

Priory Junior School uses CCTV in locations around the school site for safety, security and the prevention and investigation of incidents. CCTV images are personal data where individuals can be identified and will be processed in accordance with this policy and ICO guidance.

- cameras will be positioned and used proportionately for defined purposes;
- clear signage will indicate where CCTV is in operation;
- access to live and recorded images will be restricted to authorised people with a legitimate need;
- recordings will be retained only for as long as necessary in accordance with the school's retention arrangements, unless required for an incident, safeguarding matter, investigation or legal purpose;
- disclosures to police, insurers, legal advisers or other third parties will only be made lawfully and securely; and
- requests for access to CCTV images will be handled as data protection rights requests where applicable.

CCTV enquiries should be directed to the DPO, Samantha Ford, via the school office.

14. Photographs and videos

The school may take photographs and videos for educational activities, assessment, record-keeping, displays, newsletters, the school website, social media and publicity. The lawful basis will depend on the purpose.

- For routine educational and school-management purposes, the school may rely on public task or another appropriate lawful basis.
- For external publicity, marketing or promotional use where consent is the appropriate basis, the school will obtain clear parent/carer consent and explain how the image will be used.
- Where consent is relied upon, it may be withdrawn. The school will stop future use and take reasonable steps to remove the image from school-controlled digital platforms. It may not be possible to recall material already lawfully printed, distributed or published by third parties.
- Images will not normally be accompanied by unnecessary personal information that increases identification or safeguarding risk.
- Parents/carers taking photographs or videos for their own personal use at school events are generally outside data protection law, but the school may set safeguarding restrictions and asks that images of other children are not published online without appropriate agreement.

Staff must use school-authorised devices, accounts and storage for school photographs and videos unless a specific alternative has been approved.

15. Artificial intelligence, automated decision-making and EdTech

15.1 Generative AI

Priory recognises that generative AI can support education and administration, but it can also create significant privacy, accuracy, security and safeguarding risks. Only school-approved AI tools may be used for school business.

- Personal data, special category data, safeguarding information, confidential staff information or identifiable pupil work must not be entered into public or unapproved AI tools.
- Before an approved AI tool is used with personal data, the school will establish a lawful basis, understand how the provider uses and retains prompts/outputs, check whether data is used to train models, assess international transfers and security, and update privacy information where necessary.
- A DPIA will be completed where AI use is likely to result in high risk, including profiling, monitoring, significant automated decisions or new large-scale processing.
- Age restrictions and terms of service will be checked before pupils are given direct access to an AI service.
- AI outputs must be checked by a competent person for accuracy, bias and appropriateness. AI must not be treated as an authoritative source simply because it produces a confident answer.
- Entering personal data into an unauthorised AI tool must be reported immediately as a potential data breach so the DPO can assess the risk and necessary action.

15.2 Automated decision-making and profiling

The DUAA expands the circumstances in which significant decisions may be made solely by automated processing. Priory will not use solely automated processing to make a decision that has a legal or similarly significant effect on a pupil, parent/carer or staff member unless the DPO has confirmed that the processing is lawful and appropriate safeguards are in place. Those safeguards include informing the individual about the decision and enabling representations, human intervention and challenge. Additional restrictions apply to special category data.

15.3 Procuring EdTech and online services

Before adopting a new digital service, app, platform, monitoring solution or cloud tool that will process personal data, the school will undertake proportionate due diligence. This will include consideration of:

- what personal data is collected and whether it is necessary;
- controller/processor roles and a compliant written contract;
- security, access controls, breach notification and deletion/return of data at contract end;
- retention periods, sub-processors and international transfers;
- whether the service is likely to be accessed by children and the additional protections required;
- whether a DPIA is required; and
- whether privacy notices, acceptable use arrangements or staff/pupil training need to be updated.

16. Filtering and monitoring

The school uses filtering and monitoring arrangements to provide a safe online environment and meet safeguarding responsibilities. Monitoring data can itself be personal data and may include website activity, searches, prompts, chat conversations, images or alerts associated with a user or device.

- access to monitoring data and alerts will be limited to authorised staff with an appropriate safeguarding and operational need;
- staff with access will receive appropriate training, including safeguarding and online safety;
- processing will be lawful, proportionate and transparent, and relevant privacy notices will explain what is monitored, why, who can access it and how long it is retained;
- a DPIA will be completed before introducing a new monitoring system or making a significant change where required; and
- where automated or AI-based monitoring is used, human review and appropriate safeguards will be applied before significant action is taken.

17. Data protection by design and default

Data protection will be considered from the start of projects and changes, not added afterwards. The school will:

- only collect and use the minimum personal data required;
- build privacy and security settings into systems by default;
- complete DPIAs before processing likely to create a high risk to individuals, including significant new technology, monitoring, AI, biometrics or large-scale sensitive processing;
- consult the DPO early enough for advice to influence the design;
- use pseudonymisation or anonymisation where appropriate;
- ensure privacy notices, contracts, retention and access controls are updated when processing changes; and
- review new processing after implementation where risks or circumstances change.

18. Data security and storage

The school will take appropriate technical and organisational measures to protect personal data against loss, misuse, unauthorised access, disclosure or alteration. Security expectations include:

- personal data is stored only in approved school systems, secure cloud services and designated physical locations;
- school accounts are used for school business; staff must not forward work personal data to personal email accounts;

- users have unique accounts and only the access needed for their role; access is removed promptly when roles change or staff leave;
- passwords/passphrases are strong and unique. Systems will use appropriate technical controls, and NCSC-style machine-generated passwords or random-word passphrases are preferred;
- multi-factor authentication will be enabled for staff cloud services, remote access and IT administrative accounts in line with DfE cyber security standards where the service supports it;
- screens are locked when unattended and devices are physically protected;
- portable devices and removable media containing personal data are encrypted; unapproved USB/removable media must not be used;
- paper records containing confidential information are kept secure and are not left in classrooms, offices or staff areas where unauthorised people can access them;
- where personal data must be taken off site, this will be limited to what is necessary and protected in accordance with school procedures;
- email recipients and attachments are checked carefully before sending; BCC or approved mailing systems are used where appropriate for group communications; and
- sensitive personal data shared externally is protected using an appropriately secure method. Where a password is used to protect a file, the password is communicated separately.

Staff must immediately report lost devices, suspected compromised accounts, phishing, malware, ransomware or other cyber incidents. Cyber security and data protection incidents may overlap and will be managed together where appropriate.

19. Retention and disposal

Personal data will be kept only for as long as it is needed for the purpose for which it was collected, to meet legal requirements, or for an established school business need. The school will follow its records retention schedule and applicable statutory or sector guidance.

- retention periods will be recorded and reviewed;
- duplicate and temporary copies will be deleted when no longer required;
- paper records will be shredded or otherwise securely destroyed;
- electronic records will be securely deleted, overwritten or anonymised as appropriate;
- when a third party disposes of records for the school, the school will obtain appropriate contractual assurances; and
- safeguarding and child protection records will be retained and transferred in accordance with safeguarding requirements and the Child Protection Policy.

20. Personal data breaches and cyber incidents

A personal data breach can be accidental or deliberate. Staff must report a breach or suspected breach immediately - they must not wait until all facts are known. Examples include:

- an email, attachment, letter or report sent to the wrong person;
- loss or theft of a device, USB drive, paper file or photograph containing personal data;
- unauthorised access to CPOMS, the MIS, email, cloud storage or another school system;
- phishing or compromised login credentials;
- publication of personal information on the website or social media in error;
- safeguarding or medical information being accessed by an unauthorised person;
- personal data entered into an unauthorised AI service or other online tool; or
- ransomware, malware or another cyber incident that affects the confidentiality, integrity or availability of personal data.

The DPO will assess whether the incident is a personal data breach, contain and mitigate the risk, document the decision, and determine whether notification to the ICO and/or affected individuals is required. Where notification to the ICO is required, it must be made without undue delay and, where feasible, within 72 hours of the school becoming aware of the breach.

The detailed response process is set out in Appendix 1.

21. Data protection complaints

Anyone who believes Priory Junior School has not complied with data protection law in the way it has handled personal data has the right to complain to the school. Complaints do not need to quote legislation or use legal terminology.

A data protection complaint can be made to the DPO via office@priory-jun.notts.sch.uk, by telephone on 0115 952 6100, or in writing to the school address, marked for the attention of the Data Protection Officer.

On receiving a data protection complaint, the school will:

- provide a clear and accessible route for the complaint and reasonable assistance where needed;
- acknowledge the complaint within 30 days of receipt;
- make appropriate enquiries and investigate the substance of the complaint;

- keep the complainant informed about progress where the investigation is ongoing; and
- inform the complainant of the outcome without undue delay, including any action the school will take.

If the complainant remains dissatisfied, they may raise the matter with the Information Commissioner's Office (ICO). Where a complaint also concerns another school matter, the data protection aspects may be considered alongside the school's Complaints Procedure, but the statutory data protection complaint requirements in this section still apply.

22. Training, monitoring and review

All staff and governors will receive data protection awareness as part of induction and refresher training. Staff handling higher-risk data or systems will receive additional role-appropriate training. Cyber security, AI, safeguarding information sharing and breach reporting will form part of ongoing awareness where relevant.

The DPO will monitor implementation of this policy and may carry out audits, sampling, breach trend analysis and reviews of privacy notices, contracts and DPIAs. Significant issues will be reported to the Headteacher and Governing Body.

This policy will be reviewed at least annually and sooner where there is a significant change in law, DfE/ICO guidance, technology, school practice, a serious incident or a change in the school's legal status/data controller.

23. Linked policies and documents

- Child Protection Policy 2026/27;
- Child-on-Child Abuse Policy 2026/27;
- Online Safety / Acceptable Use arrangements and Filtering and Monitoring procedures;
- Staff Code of Conduct / Staff Handbook;
- Communications Policy;
- Complaints Procedure 2026/27;
- Visitors and VIP Policy 2026/27;
- Supporting Pupils with Medical Conditions and Administration of Medicines Policy 2026/27;
- Educational Visits Policy 2026/27;
- Health and Safety Policy;
- Freedom of Information publication scheme;
- Privacy notices;
- Records management and retention schedule; and
- any school or Local Authority cyber security, information security and acceptable use procedures.

Appendix 1: Personal data breach procedure

A. Immediate actions by the person discovering the incident

1. Stop the disclosure or loss if this can be done safely. For example, remove public access to a document, secure a device, or ask a mistaken recipient not to open, copy, forward or retain information.
2. Do not delete evidence, wipe devices, conceal the mistake or attempt a complex technical fix without advice.
3. Notify the DPO immediately and provide the facts known: what happened, when, what data is involved, whose data is affected, who may have received/accessed it, and what action has already been taken.
4. If the incident is a cyber incident, contact the school's IT support through the agreed emergency route as well as the DPO. If there is an immediate safeguarding risk, contact the DSL at once.

B. DPO assessment and containment

The DPO will coordinate the response and, with appropriate staff/IT support, will:

- determine whether there has been a personal data breach;
- contain the incident and recover/secure information where possible;
- establish the categories and approximate number of people and records affected;
- identify the type and sensitivity of data, including safeguarding, medical, special category or criminal offence data;
- assess likely consequences for individuals and the likelihood and severity of harm;
- consider whether the data was encrypted, pseudonymised or otherwise protected;
- document decisions, evidence and mitigation actions; and
- brief the Headteacher and Chair of Governors where the breach is significant or reportable.

C. Notification decisions

The DPO will determine whether notification is required. The school will:

- notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of a breach that is likely to result in a risk to individuals' rights and freedoms;
- provide the ICO with the required information and follow up with additional information as soon as possible if all details are not yet available;
- inform affected individuals without undue delay where the breach is likely to result in a high risk to their rights and freedoms, unless a legal exception applies; and
- notify other appropriate parties - for example the Local Authority, IT provider, police, insurer, safeguarding partners or Report Fraud - where the circumstances require it.

D. Recording and learning

Every personal data breach will be recorded whether or not it is reported to the ICO. The record will include the facts, cause, effects, risk assessment, decisions, notifications and remedial action. The DPO and Headteacher will review serious incidents promptly and review breach trends periodically to identify changes needed to systems, training, contracts or procedures.

Examples of first response

Incident	Immediate response
Misdirected email	Contact the unintended recipient promptly, request secure deletion, consider recall if available, preserve evidence and tell the DPO. Do not assume recall has worked.
Lost school device	Report immediately to the DPO and IT support. Record whether the device was encrypted, locked, remotely manageable and what data/accounts were accessible.
Compromised account / phishing	Change/disable credentials through IT support, revoke sessions/tokens where possible, enable containment controls, check mailbox forwarding rules and report to the DPO.
Safeguarding data disclosed	Tell the DPO and DSL immediately. Consider safeguarding risk to the child/person as well as data protection risk.
Personal data entered into unauthorised AI	Stop further use, record the tool/account/data entered and whether history can be deleted, tell the DPO and IT lead, and assess provider retention/training risks.
Paper record missing	Search proportionately without disclosing further information, identify what the record contains and who may access the location, and report to the DPO immediately.

Appendix 2: Staff quick guide - protect personal data

Area	Staff expectation
Email	Use school email. Check recipients and attachments. Use BCC for group messages where appropriate. Do not forward school personal data to a personal email account.
Passwords	Use unique, strong passwords/passphrases. Never share credentials. Report suspected compromise immediately.
Screens and devices	Lock the screen when you step away. Keep devices secure. Use school-approved storage and MFA where provided.
Paper	Keep confidential papers out of public view. Lock them away when not in use. Dispose of them through confidential waste/shredding.
Photos/videos	Use approved devices and school storage. Check the purpose and relevant permission/lawful basis before publication.
AI	Do not enter personal, safeguarding, medical or confidential information into an unapproved AI tool. Report accidental entry immediately.
Requests for information	Any request for “my information”, “everything you hold about me” or similar may be a SAR. Forward it to the DPO immediately.
Safeguarding	Share necessary information with the DSL or appropriate agencies when required to keep a child safe. Data protection is not a reason to withhold urgent safeguarding information.
Mistakes	Report them immediately. Prompt reporting gives the school the best chance to contain the impact and meet legal deadlines.