Data Protection Policy

Document Control Page

Revision History

Date	Type of change	Initials	Purpose of Revision
September 2018	Major	AR	Reflecting changes re GDPR
September 2019	Minor	MM	Date changed in footer
September 2020	Minor	MM	Date changed in footer
September 2021	Minor	MM	Date changed in footer
September 2022	Minor	KS	Date changed in footer
November 2023	Minor	KS	Date changed in footer
December 2024	Minor	KS	Date changed in footer
September 2025	Minor	MP	Date change and DPO Name change.
October 2026	Major	MP	2026 legislation and guidance review. For governor approval.

Hatch Warren Infant School

Data Protection Policy

Introduction and scope

The school collects and uses personal data to provide education, safeguard children, employ staff and carry out its associated functions. This policy explains how everyone working for the school must handle that information lawfully and securely.

The school is the data controller for personal data it processes for its own purposes. Other organisations may be independent controllers for information they

receive. This policy applies to staff, governors, volunteers and contractors, and to paper records, electronic systems, images, recordings, emails and messages.

Legal framework

The school complies with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations 2003, as amended by the Data (Use and Access) Act 2025. The 2025 Act amends these laws; it does not replace UK GDPR.

Most remaining data protection reforms commenced on 5 February 2026. The requirement for organisations to have a data protection complaints process commenced on 19 June 2026. The school also follows applicable education and safeguarding legislation and current ICO and Department for Education guidance.

Personal data and protection principles

Personal data is information relating to an identified or identifiable living person. Examples include names, contact details, attendance, photographs, staff records and financial information. Pseudonymised information remains personal data if a person can be identified using additional information.

The school processes data lawfully, fairly and transparently; uses it for specified and compatible purposes; collects only what is necessary; maintains accuracy; keeps it only as long as necessary; and protects its confidentiality, integrity and availability. The school must be able to demonstrate compliance with these principles.

Responsibilities and the Data Protection Officer

The Governing Body oversees compliance and the Headteacher ensures suitable procedures, resources and training. All staff must follow this policy, protect information, recognise rights requests and report incidents immediately.

The policy names Maria Pouney as Data Protection Officer (DPO), contactable at dpo@hwis.hants.sch.uk. The DPO advises, monitors compliance, advises on impact assessments and acts as contact for individuals and the ICO. The school remains responsible for its processing decisions.

The DPO must act independently, report to the highest management level and have suitable expertise, time and resources. Other duties must not involve determining the purposes and means of processing in a way that creates a conflict. The

Governing Body must review and document the suitability of the appointment and any conflicts.

Lawful processing and sensitive information

The school identifies and records an Article 6 lawful basis before processing. Core education and safeguarding activities normally rely on public task or legal obligation, with the relevant legal underpinning recorded. Contract, vital interests or consent may apply to particular activities where their conditions are met.

Consent must be freely given, specific, informed and unambiguous, recorded and capable of withdrawal. It is not used where individuals have no genuine choice. Withdrawal does not affect earlier lawful processing. Optional publicity photographs are considered separately from information needed for education or safeguarding.

The 2025 Act introduced recognised legitimate interest as an additional lawful basis. As a public authority, the school cannot use either legitimate interests or recognised legitimate interest when performing its public tasks. Any proposed use outside those tasks requires DPO advice and documented justification.

Special category data includes health, racial or ethnic origin, religious beliefs and biometric data used for unique identification. Processing requires both an Article 6 basis and an Article 9 condition, with relevant Data Protection Act Schedule 1 conditions and an appropriate policy document where required. Criminal offence and DBS information require Article 10 authority or an applicable statutory condition. Access is strictly limited.

Privacy information

The school provides accessible privacy notices for pupils and parents, staff and other relevant groups. These explain controller and DPO details, purposes and lawful bases, recipients, international transfers, retention, rights and how to complain. Notices are provided when data is collected, or within the applicable period for indirectly obtained data, subject to lawful exceptions.

Notices are reviewed when systems, suppliers, purposes or sharing arrangements change. Children receive information suited to their age and understanding.

Sharing information and safeguarding

Data protection law enables appropriate safeguarding information sharing. Staff must promptly refer concerns to the Designated Safeguarding Lead (DSL), share relevant information securely with authorised recipients and record what was shared, with whom, why and under which lawful basis. Consent is not required where another lawful basis applies.

From 30 September 2026, section 16LA of the Children Act 2004 imposes an information sharing duty on relevant organisations. Where it applies, relevant information must be shared with another relevant person if and insofar as it may facilitate their safeguarding or welfare functions, unless sharing would be more detrimental to the child than not sharing. Staff must follow current statutory guidance and seek prompt DSL advice on the limited exception.

Confirm recipients and disclose only appropriate information. Explain sharing to families where safe and appropriate. Record decisions not to share and their reasons. DPO advice or the absence of a data sharing agreement must not delay urgent safeguarding action. Routine sharing arrangements are documented.

Individual rights and access requests

Individuals have rights to information, access, rectification, erasure, restriction, portability and objection, and safeguards for significant automated decisions, subject to the conditions and exemptions applying to each right. For example, erasure is not absolute where records must be retained by law.

Requests may be made verbally or in writing to any member of staff and do not need to mention UK GDPR or use a particular form. Staff must forward them immediately to the DPO, who records the receipt date, checks identity or representative authority only where necessary, and calculates the deadline.

The school responds without undue delay and normally within one calendar month. School holidays do not stop this period. For complex requests or a number of requests from the same individual, the period may be extended by up to two further months; the individual must be told within the initial month and given reasons.

For a subject access request, clarification is sought promptly only where reasonably required to identify the information or processing activities requested. The response clock pauses on the day clarification is requested and resumes the day

after it is received. The school records the pause and revised deadline, and does not force an individual to narrow a request.

Searches must be reasonable and proportionate. The DPO documents the systems searched and reasons for any limits. A large volume of data is not, by itself, a reason to refuse a request. Responses are normally free; any fee or refusal for a manifestly unfounded or excessive request, or fee for further copies, requires documented justification and DPO review.

The school protects third-party information and applies exemptions individually, rather than withholding entire safeguarding or staff records automatically. Any refusal explains the reasons where permitted, and the right to complain to the ICO and seek a judicial remedy.

Requests involving children and educational records

The right of subject access belongs to the child. Before responding to a parent or representative, the school considers the child's understanding, authority to act, parental responsibility, court orders and the child's best interests. Parents do not have unrestricted automatic access to all information about a child or another parent.

For maintained schools in England, a parent's written request to inspect or obtain a copy of a pupil's educational record is a separate right under the Education (Pupil Information) (England) Regulations 2005, normally requiring a response within 15 school days. The DPO identifies which regime applies and handles overlapping requests appropriately, including lawful exemptions and any permitted copying charges.

Accuracy and retention

The school checks information for accuracy and distinguishes facts, professional opinions and allegations. Corrections are recorded without obscuring the history of a safeguarding record.

The school maintains and reviews a retention schedule, with category-specific periods and reasons. Staff must not retain everything indefinitely or delete records needed for an active request, complaint, investigation, litigation or safeguarding purpose. At the end of the applicable period, paper and electronic records are securely destroyed, including arrangements for backups and supplier-held copies.

Information security

Access is limited to authorised people who need information for their work. The school uses appropriate technical and organisational controls, including strong passwords, multifactor authentication where supported, managed devices, secure configuration, software updates, backups and recovery arrangements.

Paper records are stored securely; confidential conversations take place privately; screens are locked when unattended. Staff check recipients, attachments and access permissions before sending or sharing information. Bulk parent emails must not expose other recipients' addresses; use an approved communication system or BCC where appropriate.

Personal email accounts, unapproved messaging services, devices or storage must not be used for school personal data. Approved remote access and portable records require appropriate protection. Health and safeguarding details must be available to relevant staff safely, without unnecessary public display.

Personal data breaches

A personal data breach is an incident involving accidental or unlawful loss, destruction, alteration, unauthorised disclosure of, or access to personal data. Examples include misdirected emails, lost records, unauthorised system access and loss of availability following a cyber incident.

Staff must report a suspected breach immediately to the Headteacher and DPO using the school's incident procedure. If either is unavailable, escalate promptly through the school's senior leadership arrangements. Contain the incident where safe, preserve evidence and record when the school became aware; do not wait for a completed investigation.

The school assesses the likelihood and severity of risks to people. Unless a breach is unlikely to result in a risk to their rights and freedoms, the school notifies the ICO without undue delay and, where feasible, within 72 hours of awareness. This means clock hours, including weekends and holidays. Reasons for delay are recorded, and information may be supplied in phases.

Where the breach is likely to result in a high risk to individuals, they are informed without undue delay unless a lawful exception applies. The school documents every breach, the risk assessment, notification decisions, actions and lessons learned. Safeguarding risks are escalated to the DSL immediately.

Suppliers and international transfers

Before approving a supplier, the school checks its role, security, use of data, subprocessors, retention, deletion and overseas access. Processors must have an Article 28 compliant written contract and act only on authorised instructions. Independent controllers and joint controllers require appropriate sharing or responsibility arrangements.

Transfers to separate organisations outside the UK, including overseas remote access, are assessed under the UK restricted transfer rules. The EU or EEA is not treated as part of the UK. A restricted transfer requires applicable UK adequacy regulations, appropriate safeguards such as the UK IDTA or Addendum, or a valid statutory exception.

Where safeguards require a transfer risk assessment, the school documents the data protection test, assessing reasonably and proportionately whether protection after transfer is not materially lower than under UK law. The DPO checks current adequacy coverage and safeguards before approval; privacy notices describe relevant arrangements.

New systems and data protection by design

The school considers privacy, access, minimum collection and retention before introducing or materially changing processing. It maintains records of processing activities and an inventory of information assets, systems and suppliers.

A data protection impact assessment (DPIA) is completed before processing likely to create a high risk, including relevant monitoring, sensitive data or new technology. The DPO advises on the assessment; unresolved high risk requires prior consultation with the ICO. Online services likely to be accessed by children must meet applicable additional child protection design requirements, with child-friendly defaults and information.

Artificial intelligence and automated decisions

Staff must not enter identifiable pupil, parent or staff information into unapproved AI tools. Removing a name alone may not anonymise a record. Approved use requires a documented purpose, lawful basis, supplier and security checks, appropriate transparency and a DPIA where needed. The school should avoid personal data in generative AI wherever possible.

AI outputs must be checked for accuracy and bias before use. Staff remain responsible for school records and communications. An AI tool must not replace professional safeguarding judgement.

Any proposal for a decision based solely on automated processing with legal or similarly significant effects must be referred to the DPO before use. The school applies the current UK GDPR safeguards, including information about the decision, opportunities to make representations and challenge it, and meaningful human intervention. Additional restrictions apply to special category data.

Photographs communications and website technologies

The school distinguishes educational use of photographs from optional publicity. It records the appropriate lawful basis and consent where used, checks safeguarding restrictions and withdrawal requests, and controls photographer and platform access. Visitors and parents must follow the school's rules on recording and sharing images.

Operational messages to families are distinguished from direct marketing. Any marketing and use of cookies or similar website technologies must comply with PECR. Non-essential technologies require valid consent unless a specific current exemption applies and its conditions are met. A technology is not exempt simply because it is useful.

Training and monitoring

Staff and governors receive appropriate induction and refresher training, including rights requests, secure sharing, safeguarding and breach reporting. The DPO monitors compliance and reports material findings to school leadership and the Governing Body. Records include training, requests, complaints, breaches, DPIAs, contracts and retention decisions.

Data protection complaints

Anyone concerned about the school's use of their personal data can complain to the DPO at dpo@hwis.hants.sch.uk or contact the school office for help making a complaint. Complaints are accepted by email, in writing or verbally, with reasonable adjustments and assistance where needed. A particular form is not compulsory.

The school records and acknowledges receipt within 30 calendar days. It takes appropriate steps without undue delay to investigate, make relevant enquiries and

keep the complainant informed. It communicates the outcome without undue delay, explains its findings and any action or remedy, and keeps a record.

The general school Complaints Policy may support this process but must not delay or displace these data protection requirements. A complaint about the DPO's own conduct or processing decisions is referred to the Headteacher or Chair of Governors as appropriate for an impartial review.

If concerns remain, individuals may complain to the ICO at www.ico.org.uk/make-a-complaint/ or write to Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. The school explains this route in its outcome response. The complaints process does not remove an individual's right to seek a judicial remedy.

Policy review and related documents

The DPO leads an annual review, or an earlier review following legislation, significant incidents or material changes in processing. The Governing Body considers and records approval. The next scheduled review is October 2027.

Read this policy with the school's privacy notices, retention schedule, safeguarding and child protection policy, ICT security and acceptable use procedures, incident response procedure, complaints policy, photography arrangements and any applicable appropriate policy document for sensitive data.

2026 amendment summary for governors

New and updated requirements: 2026 commencement of the Data (Use and Access) Act reforms; complaints acknowledgement within 30 days and response without undue delay; reasonable and proportionate SAR searches and a justified clarification pause; updated overseas transfer test; automated decision safeguards; and the September 2026 safeguarding information sharing duty.

Existing duties made clearer: lawful bases and sensitive data conditions; DPO independence; children's and parents' access rights; breach thresholds and timescales; processor contracts; privacy notices; retention; security; DPIAs and training. AI and communication rules are practical school safeguards, rather than a claim that UK GDPR was replaced in 2026.

Before adoption, governors should confirm the DPO appointment and any conflict safeguards, arrange cover for urgent incidents, and check that privacy notices, the

retention schedule, complaints arrangements and supplier records match this policy. Record the approval date on the document control page.

Sources for the 2026 review

Official sources checked on 13 October 2026. These references support the amendments; statutory conditions and guidance must be applied to the particular processing activity.

ICO — Data (Use and Access) Act 2025 and commencement updates
https://ico.org.uk/about-the-ico/what-we-do/legislation-we-cover/data-use-and-access-act-2025/

ICO — How to deal with data protection complaints
https://ico.org.uk/for-organisations/how-to-deal-with-data-protection-complaints/

ICO — A guide to subject access
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/subject-access-requests/a-guide-to-subject-access/

ICO — Accessing pupils information
https://ico.org.uk/for-the-public/schools/pupils-info/

ICO — Data protection officers
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/data-protection-officers/

ICO — Personal data breaches a guide
https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/

ICO — A brief guide to international transfers
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/a-brief-guide-to-international-transfers/

ICO — Recognised legitimate interest
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/recognised-legitimate-interest/

Department for Education — Data protection in schools including processing, policies, responsibilities, sharing, photography, EdTech and generative AI guidance https://www.gov.uk/guidance/data-protection-in-schools

Department for Education — Information sharing duty statutory guidance September 2026 https://www.gov.uk/government/publications/information-sharing-to-safeguard-children-and-young-people

Contacts

Maria Pouney
Data Protection Officer
dpo@hwis.hants.sch.uk