The John Hampden School Wendover

Data Protection Policy

Date policy last reviewed: February 2026
Date policy to be reviewed: February 2027

Signed:

_____ Head Teacher Date _____

_____ Chair of Governors Date _____

Contents

---

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents and carers, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

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 General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

This policy also supports the school's safeguarding obligations under:

- Keeping Children Safe in Education (KCSIE) 2025 – statutory guidance which requires schools to have clear policies and procedures for protecting personal data, particularly in relation to safeguarding information, child protection records, and information sharing with other agencies

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: › Name (including initials) › Identification number › Location data › Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: › Racial or ethnic origin › Political opinions › Religious or philosophical beliefs › Trade union membership › Genetics › Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes › Health – physical or mental › Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. The data controller

Our school processes personal data relating to parents and carers, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school has paid its data protection fee to the ICO, as legally required.

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 responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 Data protection officer (DPO)

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

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

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

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

Our DPO is Jai Lablans and is contactable via the school office 01296 622629.

5.3 Headteacher

The headteacher acts as the representative of the data controller on a day-to-day 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 UK
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

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

This policy sets out how the school aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have 1 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 or another person i.e. 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 or exercise its official authority**
- The data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the school performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet 1 of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**

- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

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.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, 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.

8. Sharing personal data

Sharing personal data
We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils

8.1 Sharing data with suppliers, contractors and third-party processors
When we share personal data with suppliers, contractors or other third parties who process data on our behalf (known as "data processors"), we will ensure appropriate safeguards are in place.
Before appointing a data processor, we will:

- **Assess their suitability** by checking:
  - Their data protection policies and procedures
  - Their security measures
  - Their track record and reputation
  - References from other schools or organisations
  - Whether they have appropriate insurance
  - Their compliance with UK GDPR and Data Protection Act 2018
- **Ensure they can provide sufficient guarantees that they:**
  - Comply with UK data protection law
  - Will only process data in accordance with our instructions
  - Have appropriate technical and organisational security measures in place
  - Will assist us in responding to subject access requests and other data protection rights
  - Will notify us of any data breaches
  - Will delete or return data when the contract ends

Data processing agreements
We will establish a **written data processing agreement** with every supplier or contractor before we share any personal data with them. This agreement will set out:

- The **subject matter and duration** of the processing
- The **nature and purpose** of the processing
- The **type of personal data** being processed
- The **categories of data subjects** (e.g. pupils, staff, parents)
- The **obligations and rights** of the school as data controller
- The **processor's obligations**, including:
    - To process data only on our documented instructions
    - To ensure staff processing the data are bound by confidentiality
    - To implement appropriate security measures
    - To only engage sub-processors with our prior written consent
    - To assist us with data protection impact assessments (if required)
    - To assist us in responding to requests from individuals exercising their data protection rights
    - To delete or return all personal data at the end of the contract
    - To make available all information necessary to demonstrate compliance
    - To allow for and contribute to audits and inspections

Our audit rights

Our data processing agreements will include the right for the school (or an appointed auditor) to:

- Audit the processor's data protection practices
- Inspect their security measures
- Review their processing activities
- Request evidence of compliance
- Conduct on-site inspections (where appropriate)

We will exercise these rights proportionately, typically:

- Annually for high-risk processors (e.g. those processing safeguarding data)
- Every 2-3 years for lower-risk processors
- Following any data breach or security incident
- When renewing contracts

Sub-processors

A sub-processor is another organisation that the data processor uses to help them provide their service to us. Our data processing agreements will require processors to:

- **Obtain our prior written consent** before engaging any sub-processor
- **Provide details** of the sub-processor, including:
    - Their name and contact details
    - What processing they will carry out
    - Where they are located
    - What security measures they have in place
- **Impose the same data protection obligations** on sub-processors as we impose on them
- **Remain fully liable** to us for the performance of the sub-processor's obligations

If a processor wishes to engage a new sub-processor:

1. They must notify the DPO in writing at least **30 days in advance**
2. The DPO will assess the sub-processor's suitability
3. The DPO will either approve or object to the sub-processor
4. If approved, the processor must ensure a written agreement is in place with the sub-processor
5. The processor must provide us with a copy of this agreement (or a summary) if requested

Common examples of data processors we use:

- IT support providers
- Cloud storage providers (e.g. Google, Microsoft)
- Management information system (MIS) providers
- Payroll providers
- HR and recruitment software providers
- Communication platforms (e.g. ParentMail, SchoolComms)
- Educational software and apps
- CCTV monitoring services
- Shredding and secure disposal services
- Website hosting providers

Staff responsibilities

Staff must:

- **Only share data** with approved processors listed on our Data Processor Register (maintained by the DPO)
- **Not engage new processors** without DPO approval
- **Report any concerns** about a processor's data handling to the DPO immediately
- **Ensure contracts are in place** before sharing any data

The DPO will:

- Maintain a **Data Processor Register** listing all processors and sub-processors
- Review all data processing agreements before they are signed
- Monitor processor compliance
- Conduct or arrange audits as appropriate
- Review the register annually

We will also share personal data with law enforcement and government bodies where we are legally required to do so. We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Section 8.2: **International data transfers**

When we transfer personal data internationally

The school will only transfer personal data outside of the United Kingdom (UK) where it is necessary and appropriate to do so, and where adequate safeguards are in place to protect the data.

The UK government maintains a list of countries and territories that have been assessed as providing adequate protection for personal data. This list is regularly updated. For the current list, see the ICO's guidance on international transfers. The DPO will maintain an up-to-date list based on ICO guidance

Before transferring any personal data outside the UK, staff must:

Check if the transfer is necessary - can the same outcome be achieved without transferring data internationally?

Complete an International Data Transfer Request Form (see template below)

Submit the form to the DPO for approval

Wait for written approval before proceeding with the transfer

Keep a record of the transfer in line with this policy

The DPO will assess:

Whether the country has an adequacy decision

What additional safeguards are needed (if any)

Whether a data processing agreement is required

The risks to individuals' rights and freedoms

Whether the transfer is proportionate and necessary

Emergency situations

In exceptional circumstances where an international transfer is urgently needed (for example, a safeguarding emergency involving a pupil abroad), staff should:

Contact the DPO immediately

Explain the urgency

Transfer only the minimum data necessary

Document the transfer and the reasons for it

The DPO will review the transfer retrospectively and ensure appropriate safeguards are put in place.

Review

The DPO will maintain a log of all international data transfers and review this termly to ensure ongoing compliance.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

Confirmation that their personal data is being processed

Access to a copy of the data

The purposes of the data processing

The categories of personal data concerned

Who the data has been, or will be, shared with

How long the data will be stored for, or if this isn't possible, the criteria used to determine this period

Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing

The right to lodge a complaint with the ICO or another supervisory authority

The source of the data, if not the individual

Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

Name of individual

Correspondence address

Contact number and email address

Details of the information requested

If staff receive a subject access request in any form they must immediately forward it to the DPO.

Timescales for responding to subject access requests

The school will respond to subject access requests within 1 calendar month of receipt of the request.

What is 1 calendar month?

1 calendar month means the period from the date we receive the request until the corresponding date in the next month

For example, if we receive a request on 15 January, we must respond by 15 February

If there is no corresponding date in the next month (e.g. request received on 31 January), the deadline is the last day of the next month (28 or 29 February)

This is not 30 days - it is 1 calendar month as defined by UK GDPR

Requests received during school holidays

The 1 calendar month deadline applies regardless of whether the school is open or closed for holidays. However:

If a request is received during a school holiday, the school will acknowledge receipt as soon as reasonably practicable (usually within 3 working days of the school reopening)

We will make every effort to respond within the 1 calendar month deadline, even if this falls during a holiday period

If responding during a holiday period is not reasonably practicable (for example, because key staff are unavailable or school systems are not accessible), we will:

Contact the requester as soon as possible to explain the situation

Provide a realistic timeframe for when we will respond

Respond as soon as reasonably practicable after the school reopens

Aim to respond within 10 school days of reopening, where the 1 calendar month deadline fell during the holiday

The school will always prioritise responding within the statutory 1 calendar month deadline wherever possible. Holiday periods do not automatically extend this deadline.

Extensions to the deadline

We may extend the deadline by a further 2 months (making 3 months in total) where a request is complex or numerous. If we need to do this, we will:

Inform the individual within 1 month of receipt of the request

Explain why the extension is necessary

Provide a revised deadline

Identity verification

When responding to requests, we:

May ask the individual to provide 2 forms of identification (e.g. passport, driving licence, utility bill, birth certificate)

May contact the individual via phone to confirm the request was made

The 1 calendar month deadline begins from when we receive the request, or from when we receive the additional information needed to confirm identity, whichever is later

Provision of information

We will:

Provide the information free of charge

Provide the information in a commonly used electronic format (e.g. PDF) unless the requester has asked for hard copies

Provide hard copies if requested (we may charge a reasonable fee for additional copies)

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 child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

For pupils aged 12 and above, we will usually seek the pupil's consent before responding to a parental subject access request. If the pupil does not consent, we will consider:

The pupil's age and maturity

The nature of the personal data

Any consequences of refusing the request

Whether the pupil has sufficient understanding of their rights

The DPO will make the final decision in consultation with the headteacher and, where appropriate, the designated safeguarding lead.

9.3 Responding to subject access requests

When responding to requests, we may not disclose information for a variety of reasons, such as if it:

Might cause serious harm to the physical or mental health of the pupil or another individual

Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests

Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it

Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

Is subject to legal professional privilege

Unfounded or excessive requests

If the request is unfounded or excessive, we may:

Refuse to act on it, or

Charge a reasonable fee to cover administrative costs

We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

Withdraw their consent to processing at any time

Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)

Prevent use of their personal data for direct marketing

Object to processing that has been justified on the basis of public interest, official authority or legitimate interests

Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)

Be notified of a data breach (in certain circumstances)

Make a complaint to the ICO

Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

Timescales for other rights

The school will respond to requests to exercise other data protection rights (such as rectification, erasure, or restriction) within 1 calendar month of receipt of the request, following the same principles as for subject access requests outlined in section 9.1 above.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. Photographs and videos

Photographs and videos

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

11.1 Consent

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and the pupil.

Our consent form will specify the different ways we may use images, and parents/carers can choose which uses they consent to. These include:

Within school - in school newsletters

Outside of school - by external agencies such as the school photographer, local newspapers, promotional campaigns

Online - on our school website, social media accounts (e.g. Facebook, Instagram)

In the local media - local newspapers, community magazines

11.2 Withdrawing consent

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further. Data Protection Policy February 2026

Parents/carers or pupils can withdraw consent by:

Contacting the school office in writing (email or letter)

We will action the withdrawal as soon as reasonably practicable, and confirm this in writing.

Please note: We cannot remove images that have already been published in print (e.g. in a newspaper or yearbook that has already been distributed), but we will remove them from our website and social media, and will not use them in future.

11.3 Safeguarding and safety

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

We will:

Never use full names alongside images (e.g. we might say "Year 1 enjoying their science experiment" but not "Emily Smith enjoying her science experiment")

Never include personal details such as home addresses, email addresses, or phone numbers

Be particularly careful with images of pupils who are looked after, have a child protection plan, or where there are safeguarding concerns

Check our safeguarding records before publishing any images to ensure we don't inadvertently publish images of children who should not be identified

11.4 Parents/carers taking photographs and videos at school events

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation.

However, we ask that parents/carers:

Only take photos/videos of their own child where possible

Do not share photos/videos containing other children on social media (e.g. Facebook, Instagram, Twitter/X) unless all the relevant parents/carers have agreed to this

Do not take photos/videos during performances if this has been requested by the school (e.g. to protect children's privacy or for safeguarding reasons)

Are mindful of other children in the background of photos/videos

Respect if another parent/carer asks them not to take photos/videos of their child

We will remind parents/carers of these expectations before school events (e.g. in newsletters, on event invitations, and in announcements before performances).

If a parent/carer is concerned about another parent/carer taking or sharing photos/videos of their child, they should contact the school office or headteacher.

11.5 School photographer

We use Veronica as our school photographer.

The school photographer:

Has a written agreement with the school that complies with data protection law

Has appropriate safeguarding checks in place (DBS check)

Will only use images for the purposes we have agreed (e.g. providing photos to parents/carers)

Will not use images for any other purpose without our consent

Will securely delete images after [insert timeframe, e.g. 6 months]

Parents/carers can purchase photographs directly from the photographer. The school does not share pupil or parent/carer contact details with the photographer without consent.

12. Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT, Microsoft Copilot, Google Gemini and Claude. The John Hampden School recognises that AI has many uses to help pupils learn and support staff efficiency, but also poses risks to sensitive and personal data.

12.1 Unauthorised AI tools

An "unauthorised AI tool" is any AI system, application, or chatbot that has not been explicitly approved by the school's senior leadership team and DPO for use with school data.

Unauthorised AI tools include, but are not limited to:

Free versions of generative AI chatbots (e.g. ChatGPT, Google Gemini, Claude) accessed via public websites

AI writing assistants not approved by the school

AI image generators that are not school-approved

Any AI tool that does not have a data processing agreement in place with the school

Browser extensions or plugins with AI capabilities that have not been approved

AI tools accessed via personal devices or personal accounts

12.2 Prohibition on entering personal and sensitive data

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

Personal and sensitive data includes, but is not limited to:

Pupil names, dates of birth, addresses, or contact details

Staff personal information

Parent/carer contact details

Safeguarding information

Special educational needs information

Medical information

Assessment data that can identify individuals

Behaviour records

Attendance records

Any information that could identify a child, staff member, or family

12.3 Approved AI tools

The school has approved the following AI tools for use with school data:

The Key GPT

National College GPT

None at present - staff must seek approval before using any other AI tool with school-related information

A full list of approved AI tools and their permitted uses is maintained by the DPO and is available to all staff

12.4 Acceptable use of approved AI tools

When using approved AI tools, staff must:

Only use them for their approved purpose

Follow any specific guidance provided with the approval

Never enter personal or sensitive data unless explicitly permitted

Use anonymised or fictional examples where possible

Be aware that AI-generated content may be inaccurate and must be checked

Comply with the school's Acceptable Use Policy at all times

Further guidance on the acceptable use of AI tools can be found in our Acceptable Use Policy.

12.5 Data breach procedures

If personal and/or sensitive data is entered into an unauthorised generative AI tool, The John Hampden School will treat this as a data breach, and will follow the personal data breach procedure outlined in appendix 1.

Staff must report any suspected or actual breach immediately to the DPO.

12.6 Review

This section will be reviewed regularly as AI technology and guidance evolves. Staff will be informed of any changes via staff briefings and email updates.

13. Data protection by design and default

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

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge

- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO, and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

14. Data security and storage of records

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

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our E-safety policy / ICT policy / acceptable use agreement)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

15. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

16. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website, which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

17. Training

All staff and governors are provided with data protection training as part of their induction process.

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

18. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and approved by the full governing board.

19. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Privacy notices
- Acceptable Use Policy
- Child Protection Policy
- Photography Policy
- Online Safety Policy
- Social Media Policy

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

Step 1: Identifying and reporting a potential breach

Who is responsible for identifying breaches?

All staff members, governors, volunteers, and data processors working on behalf of the school are responsible for identifying and reporting potential data breaches. This includes:

Teaching and support staff

Senior leadership team

Administrative staff

IT support staff (internal and external)

Governors

Volunteers

Contractors and third-party service providers

What constitutes a potential breach?

A data breach occurs when personal data has been accidentally or unlawfully:

Lost

Stolen

Destroyed

Altered

Disclosed or made available where it should not have been

Made available to unauthorised people

Examples of potential breaches include:

Sending an email containing personal data to the wrong recipient

Losing a device (laptop, tablet, USB stick) containing personal data

Leaving paper records in an unsecured location

Unauthorised access to school systems

Personal data being posted on the school website in error

Verbal disclosure of personal information to unauthorised individuals

Disposing of confidential records in general waste

Entering personal data into unauthorised AI tools or applications

Internal reporting timescales

On finding or causing a breach or potential breach, the staff member, governor, volunteer, or data processor must immediately notify the data protection officer (DPO).

"Immediately" means as soon as the breach is discovered, and in any case within 1 hour during the school day, or by 9am the next school day if discovered outside school hours.

If the DPO is unavailable, report to the headteacher who will contact the DPO.

Out of hours emergency contact: If a serious breach occurs outside school hours (e.g. theft of a school laptop, major cyber incident), contact the headteacher immediately on [insert emergency contact number] who will notify the DPO.

How to report a breach:

Report the breach to the DPO by:

In person (if on school premises)

Phone: 01296 622629 (school office - ask for the DPO, Jai Lablans)

Email: [insert DPO email address]

When reporting, provide as much information as possible:

Your name and contact details

Date and time the breach occurred (or was discovered)

What happened - a brief description of the incident

What personal data was involved (e.g. pupil names, addresses, safeguarding information)

How many individuals are affected (approximate number if not known exactly)

Whether the data was encrypted or password protected

What immediate action you have taken (if any)

Important: Do not delay reporting while gathering all details. Report immediately with whatever information you have, and provide additional details as they become available.

Step 2: Initial investigation

The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

Lost

Stolen

Destroyed

Altered

Disclosed or made available where it should not have been

Made available to unauthorised people

Staff, governors, and volunteers will co-operate fully with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.

The DPO will complete their initial assessment within 4 hours of being notified (during school hours), or by 12pm the next school day if notified outside school hours.

Step 3: Containment and escalation

If a breach has occurred or it is considered likely that is the case, the DPO will immediately alert the headteacher and the chair of governors.

The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors must help the DPO with this where necessary, and the DPO will take external advice when required (e.g. from IT providers, legal advisors, or the ICO helpline).

Immediate containment actions may include:

Recalling emails sent in error

Retrieving lost or misplaced documents

Changing passwords or access credentials

Isolating affected IT systems

Contacting third parties who may have received data in error

Removing incorrectly published information from the website

(See the actions relevant to specific data types at the end of this procedure)

Step 4: Risk assessment

The DPO will assess the potential consequences of the breach, both before and after the implementation of steps to mitigate the consequences. The assessment will consider:

How serious the potential or actual impact is on individuals

How likely it is that the impact will occur

The type of data involved (e.g. safeguarding information is higher risk than general contact details)

How many people are affected

Whether the data was encrypted or password protected

Who has accessed or could access the data

What harm could result (e.g. identity theft, emotional distress, physical harm, discrimination)

Step 5: Deciding whether to report to the ICO and affected individuals

The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool.

The breach must be reported to the ICO if it is likely to result in a risk to the rights and freedoms of individuals. This includes risks such as:

Identity theft or fraud

Financial loss

Damage to reputation

Loss of confidentiality

Discrimination

Physical, material or non-material damage

The breach must be reported to affected individuals if it is likely to result in a high risk to their rights and freedoms.

The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored in the secure data breaches folder on the school server.

Step 6: Reporting to the ICO (if required)

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website (www.ico.org.uk), or through its breach report line (0303 123 1113), within 72 hours of the school becoming aware of the breach.

The 72-hour timeframe begins from when the school first became aware of the breach, not when the DPO completes their investigation.

As required, the DPO will set out:

A description of the nature of the personal data breach including, where possible:

The categories and approximate number of individuals concerned

The categories and approximate number of personal data records concerned

The name and contact details of the DPO

A description of the likely consequences of the personal data breach

A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the school's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

Step 7: Notifying affected individuals (if required)

Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing without undue delay. This notification will set out:

A description, in clear and plain language, of the nature of the personal data breach

The name and contact details of the DPO

A description of the likely consequences of the personal data breach

A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.

Step 8: Recording and documentation

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

Facts and cause

Effects

Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored [insert location, e.g. "in the secure data breaches folder on the school server, accessible only to the DPO, headteacher and chair of governors"].

Step 9: Review and lessons learned

The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen within 5 school days of the breach being contained.

The review will consider:

Root cause of the breach

Whether existing policies and procedures were followed

Whether policies and procedures need updating

Whether additional staff training is needed

Whether additional technical or physical security measures are needed

Any patterns or trends with previous incidents

The DPO and headteacher will meet at least termly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches.

A summary of data breaches (anonymised where appropriate) will be reported to the Finance, Buildings, H&S Committee annually as part of the DPO's report to governors.

Actions to minimise the impact of data breaches

We set out below the steps we will take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error and immediately notify the DPO

Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error

If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the external IT support provider to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)

In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way

The DPO will endeavour to obtain a written response from all the individuals who received the data, confirming that they have complied with this request

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

If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform local safeguarding partners

Personal data published on the school website in error

The person who discovers the breach must immediately notify the DPO and, if possible, the website administrator

The DPO or website administrator will remove the information from the website immediately

The DPO will check whether the page has been cached by search engines and take steps to request removal from search engine caches

The DPO will assess whether the information has been accessed, downloaded or shared, and take appropriate action

Loss or theft of devices containing personal data (laptops, tablets, USB drives)

The person who discovers the loss or theft must immediately notify the DPO and the headteacher

If the device is stolen, the police must be contacted and a crime reference number obtained

The DPO will work with IT support to:

Determine what data was on the device

Confirm whether the data was encrypted

Remotely wipe the device if possible

Change passwords for any accounts that may have been accessible from the device

The DPO will assess the risk based on whether the device was encrypted and password protected

Unauthorised access to school systems (cyber incident/hacking)

The person who discovers the breach must immediately notify the DPO and headteacher

The DPO will work with IT support to:

Isolate affected systems to prevent further unauthorised access

Assess what data may have been accessed or compromised

Change all relevant passwords

Review access logs if available

Consider whether to report to Action Fraud and the National Cyber Security Centre

The headteacher may decide to close affected systems until security is restored

Personal data entered into unauthorised AI tools

The person who discovers or commits the breach must immediately notify the DPO

The DPO will:

Identify what data was entered and into which AI tool

Review the AI tool's privacy policy and data retention practices

Contact the AI provider (if possible) to request deletion of the data

Assess whether the data may have been used to train the AI model

Consider whether affected individuals need to be notified

The headteacher will decide whether additional staff training is required

Other types of breach that could occur:

Details of pupil premium interventions for named children being published on the school website

Non-anonymised pupil assessment results or staff pay information being shared with governors

Hardcopy reports sent to the wrong pupils or families

Confidential documents left in an unsecured location (e.g. on a desk, in a classroom, in a photocopier)

Verbal disclosure of personal information to unauthorised individuals

Disposal of confidential records in general waste bins

For all breaches, the key principles are:

Report immediately - don't delay

Contain quickly - stop the breach getting worse

Assess the risk - understand the potential impact

Take action - protect affected individuals

Learn lessons - prevent it happening again

Appendix 2: Record Retention Schedule

This schedule sets out how long we will keep different types of records, in line with legal requirements and best practice guidance.

General principles:

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. Data Protection Policy February 2026

Legal basis for retention periods:

Our retention periods are based on:

Legal requirements (e.g. employment law, tax law, safeguarding requirements)

Limitation periods for legal claims

Best practice guidance from the Information and Records Management Society (IRMS)

Guidance from the Information Commissioner's Office (ICO)

What happens when the retention period expires:

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law. Data Protection Policy
February 2026