Hartismere School

Data Protection Policy

Policy No 5

Policy led by: AJS Reviewed: March 2024 Next review: March 2026

Contents

1. Aim

Hartismere aims to ensure that all personal data collected about staff, pupils, parents, governors and other individuals is collected, stored and processed in accordance with UK data protection law. This applies to all personal data, regardless of whether it is in paper or electronic format.

The school's Privacy Notice details the categories of data we collect from members of the school community, the lawful bases for collecting this information, data retention guidelines, with whom we may share data and why, and the school's procedures for requesting access to personal data (Subject Access Request). A copy of the Privacy Notice is available on the school's website, or in paper format from the school Reception.

2. Legislation and Guidance

This policy has been informed by the following legislation and guidance:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA 2018)
- Protection of Freedoms Act 2012 (when referring to the use of biometric data)
- Guidance published by the Information Commissioner's Office (ICO): https://ico.org.uk/

3. Definitions

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living individual. 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 -Religious or philosophical beliefs -Trade union membership -Biometrics (such as fingerprints), 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.

TERM	DEFINITION
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 of 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

For the purposes of data protection law, Hartismere Family of Schools is the data controller for all schools in the Trust.

5. Roles and Responsibilities

This policy applies to **all staff** employed by the school and to external organisations or individuals working on the school's behalf:

Local Governing Body

The Local Governing Body has overall responsibility for ensuring that the school complies with all relevant data protection obligations. They are responsible for reviewing and approving the school's Data Protection Policy and Privacy Notice.

Data Protection Lead

The Trust's Data Protection Lead is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law, and developing related policies and guidelines where applicable.

The Data Protection Lead is the first point of contact for the ICO. They are not ultimately responsible for compliance; the school is ultimately responsible for meeting the requirements of GDPR.

The Trust's Data Protection Lead is Miss A. Stanley, based at Benjamin Britten School and contactable on data@hartismere.family, or through telephoning the school's reception on 01502 582312.

All staff

All members of teaching and support staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their own personal data, such as a change of address
- Contacting the Data Protection Lead 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 obtain consent, 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 individual
- 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 the 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

Lawfulness, fairness and transparency

The school will only process personal data where it has one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual 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, the school will also meet one 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, the school 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 the school first collects personal data directly from individuals, it will provide them with the relevant information required by data protection law.

The school will always consider the fairness of the data processing. The school will ensure it does not handle personal data in ways that individuals would not reasonably expect, or uses personal data in ways which have unjustified adverse effects on them.

Limitation, minimisation and accuracy

The school will only collect personal data for specified, explicit and legitimate reasons. The school will explain these reasons to the individuals when it first collects their data.

If the school wants to use personal data for reasons other than those given when it first obtained it, it will inform the individuals concerned before doing so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

The school 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, available here: https://irms.org.uk/page/AcademiesToolkit

8. Sharing Personal Data

The school's Privacy Notice details the circumstances in which it may share the personal data of students, staff, Governors and parents. The Privacy Notice is available on the school website or in paper format from the school Reception.

9. Subject Access Requests and other Rights of Individuals

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 the school will be able to respond to requests more efficiently if they are made in writing and include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

Alternatively, you may complete a copy of the school's Subject Access Request form available through emailing data@hartismere.family or obtaining a paper copy from the school Reception.

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 13 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 under 13 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.

Children aged 13 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, some subject access requests from parents or carers of pupils at our school may not 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.

Responding to Subject Access Requests

When responding to requests, the school:

- Will ask the requestor to provide a form of photo identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual it will comply within 3 months of receipt of the request, where a request is complex or numerous. The school will inform the individual of this within 1 month, and explain why the extension is necessary

The school may choose not to 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 the school cannot reasonably anonymise, and the school does not 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

If the request is unfounded, excessive, or vexatious, the school may refuse to act on it, or charge a reasonable fee to cover administrative costs. The school will take into account whether the request is repetitive in nature when making this decision.

When the school refuses a request, it will tell the individual why, and tell them they have the right to complain to the ICO.

Other data protection rights of the individual

In addition to the right to make a Subject Access Request, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask the school 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 which 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 Trust's Data Protection Lead. There will be some instances where it is not possible to fulfill a request, for example, the school has a legal duty to process the information.

10. Parental Requests to see the Educational Record

As the school is an academy, there is no automatic parental right of access to the educational record. It is at the school's discretion whether they choose to provide this to a parent or carer. To request access to the educational record, individuals should contact the Trust's Data Protection Lead.

11. Biometric Recognition Systems

Where the school uses biometric data as part of an automated biometric recognition system (for example, cashless catering and access to the school's buildings), it will comply with the requirements of the Protection of Freedoms Act 2012.

The school will get written consent from at least one parent or carer before it takes any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s), in which case the school will provide alternative means of accessing the relevant services for those pupils.

Parents/carers and pupils can withdraw consent, at any time, and the school will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in the processing of their biometric data, the school will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric systems, the school will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

Please note, that in the context of the Protection of Freedoms Act 2012, a 'child' means a person under the age of 18.

12. CCTV

CCTV is used in and around the school site. The school collects and processes this data under the lawful basis of 'Public Task', as it facilitates the safe and effective day-to-day operation of the school by assisting the school in its duties with respect to health and safety, safeguarding and premises maintenance for example.

There are CCTV signs placed at the entrances of the school and around the school site to ensure members of the school community are aware that they are in an area of surveillance.

Recorded CCTV footage is included in the information available under a Subject Access Request and the individual may also request that recorded images of them are erased (this will not apply if the footage is more than 30 days old as it will have already been erased).

CCTV recordings are stored in a secure cloud-based system in school and disposed of after 30 days, unless they are subject to an investigation. CCTV recordings will be shared with the police should they be required to support a criminal investigation.

The school follows the ICO's Code of Conduct on the use of CCTV. Any enquiries about the CCTV system should be directed to the Trust's Data Protection Lead.

13. Photographs and Videos

As part of school activity, we may photograph or video record students.

For children under the age of 13:

The school will obtain written consent from parents/carers for photographs and video recordings to be taken of their child. The school will clearly explain how the photograph and/or video recording will be used.

For children over the age of 13:

The school will obtain written consent from pupils for their photograph or video recording to be taken. The school will clearly explain to the pupil how the photograph and/or video recording will be used. Where a pupil is over the age of 13 but cannot reasonably understand their rights over their photograph/ video recording, then consent will be sought from parents/ carers. This may apply where the pupil has significant special educational needs and/or disabilities.

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

Any photographs and video recordings taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, the school asks that photographs or video recordings which capture other pupils are not shared publicly on social media for safeguarding reasons.

14. Data security and storage of records

The school 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
- Two-factor authentication is used for staff emails. Staff and pupils are reminded that they should not reuse passwords from other sites
- Encryption software is used to protect 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

The school operates a clear-screen policy, whereby computers in use are locked if the staff member is going to be away from their desk. This includes staff members working from offices as well as classrooms.

Staff are requested to be mindful of what students in the vicinity may see on their screen or on their desk. Personal information of students or staff should not be viewed by other students.

Staff are requested to be mindful when using the school's reprographic equipment, ensuring papers or print-outs including the personal data of any member of the school community are not abandoned/ left behind, or disposed of without due care.

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 the school cannot or does not need to rectify or update it.

For example, the school will shred or incinerate paper-based records, and overwrite or delete electronic files. The school may also use a third party to safely dispose of records on the school's behalf. If it does so, the school 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, the Trust's Data Protection Lead must be informed within 24 hours after an individual becoming aware of a breach.

When appropriate, the school will report the data breach to the ICO within 72 hours after becoming aware of it.

17. Links with other policies

This policy operates in conjunction with the following Trust/ school policies:

- Data Protection Privacy Notice
- Freedom of Information Policy
- Child Protection Policy and Procedures

If you would like to discuss anything in this Data Protection Policy, please contact Miss A Stanley (Data Protection Lead) through the following contact details:

By post:	Benjamin Britten School Blyford Road, Lowestoft, Suffolk NR32 1JH
By telephone:	01502 582312
By email:	data@hartismere.family