DATA PROTECTION POLICY AND INFORMATION SECURITY POLICY

Date Agreed:	**September 2026**
Review Date:	**September 2029**

Contents

1. Aims

Our Trust 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)
- Data Use and Access Act 2025
- Human Rights Act 1998
- Freedom of Information Act 2000
- Common law duty of confidence
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Health and Safety at Work Act 1974

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. It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data. It also reflects the ICO's guidance for the use of surveillance cameras and personal information. In addition, this policy complies with our funding agreement and articles of association.

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.

TERM	DEFINITION
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 Trust processes personal data relating to parents and carers, pupils, staff, governors, visitors, and others, and therefore is a data controller.

The Trust is registered with the ICO as legally required. ICO Registration: ZB323813

5. Roles and responsibilities

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

5.1 Board of Trustees

The Board of Trustees has overall responsibility for ensuring that our Trust 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 Board of Trustees and, where relevant, report to the board their advice and recommendations on Trust data protection issues.

Each school within the Trust has a Data Protection Lead. Please refer to the individual school for the relevant contact details. The school data protection lead is responsible for overseeing the implementation of this policy in their school.

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

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

Our DPO is Darren Carpenter and is contactable via DCarpenter@hurst.education

5.3 All staff

Staff are responsible for:

- Collecting, storing, and processing any personal data in accordance with this policy
- Informing the Trust of any changes to their personal data, such as a change of address
- Contacting the School Data Protection Lead / 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 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

5.4 The Regulator

The Information Commissioner's Office is responsible for:

- Overseeing compliance with Data Protection legislation
- Supporting organisations to become compliant
- Enforcing the legal processing of data
- Investigating complaints where organisations are not compliant

Schools must register with the ICO and maintain a current record of the information it is processing, the legal basis for processing the information and who it is being shared with.

6. Data protection principles

The UK GDPR is based on data protection principles that our Trust 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 Trust 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 Trust can fulfil a contract with the individual, or the individual has asked the Trust to take specific steps before entering into a contract
- The data needs to be processed so that the Trust 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 Trust, 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 Trust (where the processing is not for any tasks the Trust 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 Trust's record retention schedule.

8. Sharing personal data

We will only share personal data where we have a valid legal basis, 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 – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors that can provide sufficient guarantees that they comply with UK data protection law
    - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service

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.

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

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

- Confirmation that their personal data is being processed
- Request 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

Much of this information is already detailed in the Trust Privacy Notices.

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 using the Trust document 'Individual Rights Request and Assessment Form'. All requests must 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.

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 Trust 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.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of 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 we will comply within 3 months of receipt of the request, where a request is complex or large in volume. We will inform the individual of this within 1 month, and explain why the extension is necessary

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

If the request is manifestly 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.

10. Parental requests to see the educational record

There is no automatic parental right of access to the educational record in academies but the Trust will review each request on a case-by-case basis. There are certain circumstances in which this right will 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. CCTV

We use CCTV in various locations around the Trust site to ensure it remains safe. We will follow the ICO's guidance for the use of CCTV, and comply with data protection principles.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the relevant school's Headteacher.

12. Photographs and videos

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

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.

Any photographs and videos taken by parents/carers at Trust events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Where the Trust takes photographs and videos, uses may include:

- Within Trust on notice boards and in Trust magazines, brochures, newsletters, etc.
- Outside of Trust by external agencies such as the Trust photographer, newspapers, campaigns
- Online on our Trust website or social media pages

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.

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.

13. 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 and Google Bard. Hurst Education Trust recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal 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.

14. 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 Trust'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 Trust 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

15. 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 Trust office
- Passwords that are at least 10 characters long containing letters and numbers are used to access Trust 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
- 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)

16. 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 Trust's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17. Personal data breaches

The Trust will take all preventable steps to hold and process individual data securely. In the unlikely event of a breach, the Trust has a data breach management process which all staff are aware of and have received appropriate training so they can recognise and react appropriately to a data breach.

All breaches of Data Protection legislation will be reported to the Trust DPO who will ensure the process is adhered to and ensure breaches are reported to the ICO where necessary, within the required 72 hours.

18. Training

All staff and governors are provided with data protection training on an annual basis.

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

19. Information Security

Information that is confidential but doesn't relate to an individual or individuals includes the following:

- Trust business or corporate records containing organisationally or publicly sensitive information
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations
- Politically sensitive information
- Information relating to security, investigations and proceedings
- Any information which, if released, could cause problems or damage to individuals, the public, the Trust or another organisation. This could be personal, financial, reputation or legal damage.

The information security policy covers the creation, acquisition, retention, transit, use, and disposal of all forms of information.

It applies to all employees, Governors, volunteers and staff of service delivery partners who handle information for which the Trust is responsible. It forms the basis of contractual responsibilities in contracts with Data Processors where reference is made to the Trust's Data Protection and Information Security Policy.

The Trust will maintain the confidentiality, integrity and security of all data ensuring it is gathered, secured, stored, shared and erased in accordance with the data protection regulation. The Trust will review its data protection policies as part of its governance process. It will also check the effective implementation of these policies through the regular Governor led Safeguarding Audits.

Information systems will be checked regularly for technical compliance with relevant security implementation standards.

Operational systems are subjected to technical examination to ensure that hardware and software controls have been correctly implemented.

20. Management of Information

The Trust will manage information in accordance with the principles and procedures within this policy and other relevant policies and standards. The following principles apply to how we handle information in the Trust:

- All identifiable personal information is treated as confidential and will be handled in accordance with the relevant legal and regulatory protocols.
- All identifiable information relating to staff is confidential except where national policy on accountability and openness requires otherwise.
- Procedures will be maintained to ensure compliance with Data Protection legislation, The Human Rights Act 1998, the common law duty of confidentiality, the Freedom of Information Act 2000 and any other relevant legislation or statutory obligation.

- Information is recorded, used and stored to protect integrity so that it remains accurate and relevant at all times.

21. Trust records

We will create and maintain adequate pupil, staff and other records to meet the Trust's business needs and to account fully and transparently for all actions and decisions. Such records can be used to provide credible and authoritative evidence where required; protect legal and other rights of the Trust, its staff and those who have dealings with the Trust; facilitate audit; and fulfil the Trust's legal and statutory obligations.

Records will be managed and controlled effectively to fulfil legal, operational and information needs and obligations in the most cost-effective manner, in line with the Trust's Records Management and Electronic Records Management policies.

22. Protection of Biometric information for children

The DfE provide guidance on the Protection of biometric information of children in Trusts and colleges under Protection of Freedoms Act 2012 and Data Protection Act 2018

The written consent of at least one parent must be obtained before the biometric data is taken from the child and used. This applies to all pupils in Trusts and colleges under the age of 18.

In no circumstances can a child's biometric data be processed without written consent. The Trust will not process the biometric data of a pupil (under 18 years of age) where:

a) the child (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data;

b) no parent has consented in writing to the processing; or

c) a parent has objected in writing to such processing, even if another parent has given written consent.

The Trust will where possible provide reasonable alternative means of accessing services for those pupils who will not be using an automated biometric recognition system.

The latest guidance published by the DfE for the implementation of this aspect of policy is available via the following link:

Protection of children's biometric information in schools - GOV.UK

23. Data in Transit

All employees, governors and volunteers are personally responsible for taking reasonable and appropriate precautions to ensure that all sensitive and confidential data is protected within the Trust and when accessed or transported outside the Trust.

- All sensitive and confidential electronic data being taken outside of its normally secure location must be encrypted.

- All non-electronic data must be transported and stored using an appropriate level of care and security.
- Data in transit should be kept to the minimum amount required to undertake the Trust's responsibilities.
- Any data loss must be reported immediately to the headteacher. Disciplinary action could be taken where employees do not follow the guidance set out in this Policy.

24. Data Use and Access Act 2025

The Data Use and Access Act 2025 (What it means for Trusts)

New legislation has been introduced to modernise how data is used and accessed. It is designed to supplement and clarify the UK GDPR and can be applied to requests received since Jan 2024. The key implications for Trusts are as follows:

- **Timescale** - the **one-month** time requirement only starts once identification has been confirmed. If the Trust needs to clarify the scope of a data search, the 'clock' is paused until clarification has been received from the data subject.
- **Scope of the search** - it has been clarified that requests for personal data must be 'reasonable and proportionate'. The Trust DPO will provide advice and guidance to assist the data subject (and the Trust) to identify what information is required. This will avoid having a scope that is so broad that it puts undue pressure on Trust resources and delays the time in which the data subject can access the data they need.
- **Information already held** - the provision clarifies the principle that the Trust does not need to send information to the requester, which they already hold or have access to. This confirms there is no requirement to send copies of emails that were communicated to and from the requester.
- **Data Protection Complaints procedure** - the Trust must have a dedicated data protection complaints procedure. Complaints about how the Trust has managed its data protection must be acknowledged within 30 days and should be processed without undue delay.

  The Trust's Data Protection Complaint Procedure will be managed by its DPO. The complaints procedure can be found on the DPO website (RSimmonsLtd.com, or by following the link below: Making a complaint | Roger Simmons Limited

  The DPO will support the Data Protection Complaint procedure in respect to the Trust and the data subject. In the first instance the data subject should read the 'Making a Data Protection Complaint about a Trust' on the DPO website. A complaint can then be made via a Microsoft Form or via a downloadable word document.

25. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed regularly and approved by the Board of Trustees.

Document History:

Data Protection Policy	
Policy Type:	Statutory – Trust Policy
Policy Source:	The Key and Roger Simmons Ltd
Model Policy Approval:	HET Trust Board
Review period:	3 Years

Date Reviewed	Amendments Made	Date Model Approved by Trust Board	Next Review Due
Sept 2023	New Trust Policy	3rd October 2023	September 2026
Sept 2026	Updated legislation. New sections: 5.4 The Regulator; 17 Personal data breaches; 19 Information Security; 20 Management of Information; 21 Trust Records; 22 Protection of Biometric information for children; 23 Data in Transit; 24 Data Use and Access Act 2025	16th September 2026	September 2029