Policy Date: September 2025
Date of next review: September 2026
Owner: Bursar / Network Manager
Location: StaffHub, GgovernorHub, Website

Heath Mount School

Data Protection Policy

Contents

Data Protection Policy Statement

Why this is important

Heath Mount School ("The School") is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with data protection legislation. We process personal data about our employees, students, suppliers and other individuals for a variety of business purposes. This policy sets out how we seek to protect personal data and ensure that our staff understand the rules governing their use of the personal data to which they have access during their work. This policy requires staff to ensure that the Data Protection Lead be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

The School is required to evidence how the organisational and technical measures it puts into place support the development of a culture of data protection.

The School is required to evidence where its policies, processes and procedures have not been followed and take action against individuals who do not comply so that their behaviour is dissuasive to others.

Who this policy applies to

This Policy is primarily aimed at staff: it describes how, as a matter of good practice and policy, any personal data controlled and processed by the School – including parents, pupils, contractors and colleagues (past, present or prospective) – should be handled in accordance with law and best practice. Where such staff are concerned, this Policy will inevitably therefore have some overlap or interaction with other policies concerning how staff handle data.

Supporting documentation to be read in conjunction with this policy

This policy should be read in conjunction with:

- Privacy Notice
- CCTV Policy
- Digital Media for External Use Policy
- AI Policy
- Information Rights Policy
- Data Incident and Breach Policy and Procedure

This policy applies to anyone who handles personal and/or special category data or information on behalf of Heath Mount School, whether this is paper-based, electronic or in any other formats including spoken information.

Employees are personally responsible at all times for the personal and/or special category data, in whatever format, in their care. They must safeguard the security of personal and/or special category data for which they are responsible or which they access, to carry out their work.

The School will enforce this policy through its procedures and policies and provide regular training. Breaches of this policy could lead to disciplinary action and penalties up to and including dismissal, depending on the breach and its impact on the school and data subject(s).

Key Definitions:

Personal information (or 'personal data'): any information relating to a living individual (a data subject) who can be identified from that information or from any other

information we may hold. That is not simply a name but any form of identifier, digital or contextual, including unique ID numbers, initials, job titles or nicknames. Note that personal information will be created almost constantly in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings). The definition includes expressions of opinion about the individual or any indication of the School's, or any person's, intentions towards that individual.
The personal data gathered may include but is not limited to: individuals' phone number, email address, IP address, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, family make-up, dependents, next of kin, health information and images.
Data subjects are all individuals about whom we hold Personal Information.
Special categories of personal data – are more sensitive and include data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and medical conditions (physical and/or mental health), sex life or sexual orientation, genetic or biometric data used to identify an individual. There are also separate rules for the processing of personal data relating to criminal convictions and offences.
Processing means virtually anything done with personal information, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it.
Data controller – a person or body that determines the purpose and means of the processing of personal data, and who is legally responsible for how it is used. For example, the School (including by its [trustees/directors/governors]) is a controller. An independent contractor who makes their own such decisions is also, separately, likely to be a data controller.

Data Protection Principles
Heath Mount School Trust Ltd ("The School") has a legal duty to ensure that all personal and sensitive information we process is managed in line with the principles set out in data protection law.

We will comply with GDPR which sets out six principles relating to the processing of personal data which must be adhered to by data controllers (and data processors). These require that personal data must be:

1. Processed lawfully, fairly and in a transparent manner;
2. Collected for specific and explicit purposes and only for the purposes it was collected for;
3. Relevant and limited to what is necessary for the purposes it is processed;
4. Accurate and kept up to date;
5. Kept for no longer than is necessary for the purposes for which it is processed; and
6. Processed in a manner that ensures appropriate security of the personal data.

The GDPR's broader 'accountability' principle also requires that the School not only processes personal data in a fair and legal manner but that we are also able to demonstrate that our processing is lawful. This involves, among other things:

- keeping records of our data processing activities, including by way of logs and policies;
- documenting significant decisions and assessments about how we use personal data (including via formal risk assessment documents called Data Protection Impact Assessments); and
- generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how our Privacy Notice(s) were updated; when staff training was undertaken; how and when any data protection consents were collected from

individuals; how personal data breaches were dealt with, whether or not reported (and to whom), etc.

Principle One: Lawfulness, Fairness & Transparency

In order to comply with this principle, we will ensure that we only process personal data where we are lawfully permitted to do so. We will be open and honest with individuals about the data we collect, why we use it, and which lawful basis justifies that use. We will do this via privacy notices, whether or not we collect information directly from the individuals concerned.

In addition, for each processing activity that we undertake, we will consider how that processing affects the individuals concerned.

Lawful basis for processing data

We must establish a lawful basis for processing data. Ensure that any data we are responsible for managing has a recorded lawful purpose. At least one of the following conditions must apply whenever we process personal data:

- Consent: Where necessary we hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.
- Contract: The processing is necessary to fulfil or prepare a contract for the individual.
- Legal obligation: We have a legal obligation to process the data (excluding a contract).
- Vital interests: Processing the data is necessary to protect a person's life or in a medical situation.
- Public function: Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.
- Legitimate interest: The processing is necessary for our legitimate interests. This condition does not apply if there is a good reason to protect the individual' s personal data which overrides the legitimate interest.

Deciding which processing condition to rely on

Our commitment to the first Principle requires us to document this process and show that we have considered which lawful basis best applies to each processing purpose, and fully justify these decisions.

We must also ensure that individuals whose data is processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. We do this via a privacy notice. This applies whether we have collected the data directly from the individual, or from another source.

Privacy notices are linked to the information populated in data mapping. Our privacy notice is available from our website at or by contacting the School.

Special categories of personal data

Previously known as sensitive personal data, this means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination.

In most cases where we process special categories of personal data we will require the data subject's explicit consent to do this unless exceptional circumstances apply, or we are required to do this by law (e.g. to comply with legal obligations to ensure safeguarding).

Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

The condition for processing special categories of personal data must comply with the law. If we do not have a lawful basis for processing special categories of data than processing activity must cease.

Additionally to establishing a lawful basis for processing personal information we must also establish a lawful basis for processing special category data. At least one of the following conditions must apply whenever we process special category data (Article 9):

Explicit Consent

- Employment, social security and social protection law
- Vital interests
- Legitimate activities
- Made public by data subject
- Establishment, exercise or defence of legal claims
- Public interest on the basis of Union or Member State law
- Health or social care
- Public interest in the area of public health
- Public interest in the area of archiving, scientific or historical research or statistical purposes.

Principle Two: Purpose Limitation

In order to comply with this principle, we will only process personal data for the specific lawful purposes set out in our Record of Processing Activity and Privacy Notices, unless we are specifically permitted to process the data by law.

Principle Three: Data minimisation

In order to comply with this principle, the data we collect will be sufficient to fulfil the purpose of collection (adequate), there will be a rational link between that data and the purpose (relevant), and we will only collect the personal data we need to fulfil the specific purpose we have collected the data for.

Principle Four: Accuracy

In order to comply with this principle, we will ensure that all personal data is kept up-to-date and is accurate. We have appropriate processes in place to check the accuracy of the data we collect, and the sources of data are always recorded. We will also comply with an individual's right to rectification (see below), and we will carefully consider any challenges to the accuracy of the personal data.

Principle Five: Storage Limitations

In order to comply with this principle, we will only keep personal data for as long as we need it, and we will take all reasonable steps to destroy or erase all data that is no longer required. Personal data will be kept in accordance with our retention policy to ensure that data is not kept any longer than necessary and we will ensure that individuals understand the duration for which their personal data will be held.

Principle Six: Integrity and confidentiality

In order to comply with this principle, we will ensure that we have appropriate organisational and technical measures in place to safeguard the security of the personal data we process. This includes ensuring the confidentiality, integrity, and availability of the systems and services used to process the personal data.

Accountability and transparency

The School must ensure accountability and transparency in all our use of personal and sensitive data. To do this we must evidence we comply with each of the 6 Principles. We do this by:

- Implementing all appropriate technical and organisational measures
- Maintaining up to date and relevant documentation on all processing activities
- Conducting Data Privacy Impact Assessments (where necessary)
- Implementing measures to ensure privacy by design and default, including:
    - Data minimisation
    - Pseudonymisation / anonymisation
    - Transparency
    - Informing individuals of the processing of their information Monitoring our responsibilities in relation to https://ico.org.uk/for-organisations/accountability-framework

Data Controller

As a Data Controller, we must maintain our appropriate registration with the relevant supervisory authority e.g. Information Commissioner's Office (ICO) in the UK to continue lawfully processing data.

The School's ICO registration number is ZA145510

The data protection legislation provides that our responsibilities as data controller are to:

- Analyse and document the type of personal data we hold
- Ensure compliance with the rights of the individual
- Identify the lawful basis for processing data
- Ensuring consent procedures are lawful
- Implementing and reviewing procedures to detect, report and investigate personal data breaches
- Store data in safe and secure ways
- Assess the risk that could be posed to individual rights and freedoms should data be compromised

All staff must ensure that they:

- Fully understand their data protection obligations by attending relevant training
- Any new processing activities they are dealing with complies with our policy and are justified
- Do not use data in any unlawful way
- Do not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through their actions
- Comply with this policy at all times
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations to the DPL without delay

Roles and Responsibilities

Data Protection Lead (responsible person)

- Keeping the Governors updated about data protection responsibilities, risks and issues;
- Reviewing all data protection procedures and policies on a regular basis;

- Arranging data protection training and advice for all staff members and those included in this policy;
- Answer questions on data protection from staff, governors and other stakeholders;
- Responding to individuals (data subject) who wish to know which data is being held on them by Heath Mount School;
- Ensuring that third parties that handle the company's data have a contracts or agreement in place regarding data processing and the data controller / data processor responsibilities;

ICT support

- Ensure all systems, services, software and equipment meet acceptable security standards;
- Checking and scanning security hardware and software regularly to ensure it is functioning properly;
- Researching third-party services, such as cloud services the school / college is considering using to store or process data.

Communications support

- Approve data protection statements attached to emails and other marketing copy;
- Coordinating with the Data Protection Lead, or responsible person to ensure all marketing initiatives adhere to relevant data protection laws and this Policy.

Data security

The School must keep personal data secure and ensure that appropriate security measures are in place to protect Personal Data against unlawful or unauthorised processing, accidental loss, destruction or misuse. Where other organisations process personal data as a service on our behalf, the data processing agreement must reflect this.

In accordance with Principle 6 (Integrity and Confidentiality):

- We will ensure the confidentiality of Personal Data by protecting it against unintentional, unlawful or unauthorised access, disclosure or theft.
- We will ensure the integrity of Personal Data by maintaining its accuracy and protecting it against accidental or unlawful alteration.
- We will ensure the availability of Personal Data by regularly testing, assessing and evaluating the effectiveness of our technical and organisational measures to ensure our systems and services can be restored and accessed in a timely manner in the event of a physical or technical incident.

Our Security measures include:

- Keeping Personal Data in paper records or on removable devices in lockable rooms, desks or cupboards and disposing of these records securely when required.
- Keeping digital Personal Data in line with our agreed policies.
- Ensuring staff members only share Personal Data they use in the course of their work with authorised personnel.
- Maintaining up to date firewalls and other IT security measures, with regular audits of our IT systems.
- Training staff on the importance of data protection and safe handling of personal data.
- Regularly auditing our governance and information management processes.

Storing data securely

In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it;

- Printed data should be shredded when it is no longer needed;
- Data stored on a computer should be in line with the School's IT policy;
- Data stored on CDs or memory sticks must be encrypted or password protected and

locked away securely when they are not being used;
- Any cloud-based system used to store data needs to be registered. Servers containing personal data must be kept in a secure location, away from general office space;
- Data should be regularly backed up in line with the school backup procedures;
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones unless the appropriate technical and organisational measures are in place;
- All servers containing special category data must be approved and protected by security software;
- All possible technical measures must be put in place to keep data secure.

Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, considering the reasons that the personal data was obtained. We do not encourage the retention of any Personal Data for any longer than necessary, in accordance with Principle 5 (Storage Limitation). We will ensure that all special category data is disposed of in a way that protects the privacy of individuals. These are reflected in our Retention Schedule (link to this document needed).

Transferring data internationally

There are restrictions on international transfers of personal data. You must not transfer personal data abroad, or anywhere else outside of normal rules and procedures without having this registered onto the data map and making the Data Protection Lead aware.

Rights of individuals (Data Subject Rights)

Individuals have a number of rights regarding the use of their Personal Data. All requests will be dealt with by our Data Protection Lead in accordance with our Information Rights Policy. We must ensure individuals can exercise their rights in the following ways:

- **Right to be informed.**
  Articles 13 and 14 of the UK GDPR specify what individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UK GDPR.

- **Right of access / Subject Access Request.**
  The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information such as who it is shared with, how long information is stored and where it has been obtained from. It helps individuals to understand how and why you are using their data, and check you are doing it lawfully.

- **Right to rectification.**
  Under Article 16 of the UK GDPR individuals have the right to have inaccurate personal data rectified. An individual may also be able to have incomplete personal data completed – although this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete data.

- **Right to erasure and how to comply.**
  Under Article 17 of the UK GDPR individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.

- **Right to data portability**
  The right to data portability gives individuals the right to receive personal data they have provided to a controller in a structured, commonly used and machine readable

format. It also gives them the right to request that a controller transmits this data directly to another controller.

- **Right to object**
  Article 21 of the UK GDPR gives individuals the right to object to the processing of their personal data. This effectively allows individuals to ask you to stop processing their personal data.
  The right to object only applies in certain circumstances. Whether it applies depends on the purposes and lawful basis for processing.
- Right in relation to and right to restrict automated profiling or decision making.

The UK GDPR has provisions on automated individual decision-making (making a decision solely by automated means without any human involvement) and profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process. The UK GDPR applies to all automated individual decision-making and profiling. Article 22 of the UK GDPR has additional rules to protect individuals if you are carrying out solely automated decision-making that has legal or similarly significant effects on them.

- Right to restrict processing. Article 18 of the UK GDPR gives individuals the right to restrict the processing of their Personal Data in certain circumstances.

Over school holidays all emails sent to privacy@heathmount.org will be automatically forwarded to 9ine Consulting who will ensure that data subject queries are considered and responded to.

Privacy notice

A privacy notice must be supplied at the time the data is obtained if obtained directly from the data subject. If the data is not obtained directly from the data subject, the privacy notice must be provided within a reasonable period of having obtained the data, which means within one month.

If the data is being used to communicate with the individual, then the privacy notice must be supplied at the latest when the first communication takes place.

If disclosure to another recipient is envisaged, then the privacy notice must be supplied prior to the data being disclosed.

Our privacy notice will include the following details:

- The name and address of our school, as the Data Controller.
- The name and contact details of our Data Protection Lead.
- The categories of Personal Data we are processing.
- The purpose or purposes we intend to use the Personal Data for.
- The legal basis for processing that Personal Data (and, where special categories of personal data are being processed, the additional processing condition allowing this).
- The recipients of any Personal Data we share or disclose.
- Details of any transfers to other countries and what safeguards are in place.
- The length of time we will retain the personal data.
- The rights Data Subjects have to access their data or limit its use or disclosure.
- The right of data subjects to complain to the Regulatory Authority about our use of their personal data.
- The source of the personal data (where we receive it from a third party).
- The existence of any automated decision-making (including profiling).

The School's privacy notice is available from our website and on request by contacting us via The School Office.

Using third party controllers and processors

As a data controller and/or data processor, we must have written contracts in place with any third-party data controllers and/or data processors that we share information with and or process information for. The contract or other legally binding agreement must contain specific clauses which set out our and their liabilities, obligations and responsibilities.

As a data controller, we must only appoint processors who can provide sufficient guarantees that they will protect the data in compliance with data protection legislation. In order to ensure our processors implement sufficient safeguards when processing personal data, we must carry out an assessment of the vendor's data protection practices.

In some circumstances we may act as a data processor. For this we must only act on the documented instructions of a controller. We acknowledge our responsibilities as a data processor under data protection legislation and we will protect and respect the rights of data subjects.

Contracts

Our contracts must comply with the standards set out by the ICO and, where possible, follow the standard contractual clauses which are available. Our contracts with data processors must set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller. These will be specified in the data processing agreements and may be further supported by a data sharing agreement and/or a privacy impact assessment.

At a minimum, our contracts must include terms that specify:

- Acting only on written instructions;
- Those involved in processing the data are subject to a duty of confidence;
- Appropriate measures will be taken to ensure the security of the processing;
- Sub-processors will only be engaged with the prior consent of the controller and under a written contract;
- The School will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under the UK GDPR;
- The processor will assist Heath Mount school in meeting its obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection ImpactAssessments; reportable here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/
- Delete or return all personal data at the end of the contract;
- Submit to regular audits and inspections and provide whatever information necessary for the School and the processor to meet their legal obligations;
- Nothing will be done by either the School or processor to infringe on the UK GDPR.

Criminal offence data / Criminal record checks

The Data Protection Act 2018 which supplements the GDPR authorises the use of criminal records checks by organisations other than those vested with official authority i.e. ICO. The Act allows Heath Mount to process criminal convictions data where necessary for the purposes of performing or exercising employment law obligations or rights. Heath Mount carry out such processing, in accordance with the principles of the Act and the school's erasure and retention policies.

The Act also authorises processing criminal records data in other circumstances, including

where the subject has given his or her consent. This would allow employers to request a criminal records check where the prospective employee agrees to this, provided that the consent meets the specific requirements under the GDPR.

All data relating to criminal offences is a special category of personal data and must be treated as such.

Audits, monitoring and training / Data audits

Regular data audits to manage and mitigate risks will inform the data mapping toolkit. This is to contain information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. We must conduct a regular data audit.

Reporting breaches

Any breach of this policy or of data protection laws must be immediately reported to the Data Protection Lead (DPL). As soon as you have become aware of a breach we have a legal obligation to report any high risk data breaches to the supervisory authority within 72 hours. Guidance can be found here https://ico.org.uk/for-organisations/guide-to- data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data- breaches/

All members of staff have an obligation to report actual or potential data protection compliance failures to the DPL. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the ICO of any compliance failures.

Any member of staff who fails to notify of a breach / incident or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal. If you have any questions or concerns about anything in this policy, do not hesitate to contact the Data Protection Lead.

Data Protection Impact Assessments

We will carry out a Data Protection Impact Assessment when the processing of personal data is likely to result in a high risk to the rights and freedoms of individuals. This process is designed to identify the nature of the risks so that mitigating actions can be taken to reduce or eliminate these risks.

We have a process in place for our staff members to follow, which includes guidance about when a Data Protection Impact Assessment is required.

Use of CCTV

The School uses CCTV in accordance with our CCTV Policy to ensure any images we collect and use are handled appropriately.

Use of Artificial Intelligence (AI)

We use high-quality educational and administrative AI tools, which we believe will enhance our students' experience at our school. AI tools are used in accordance with our AI Policy.

Monitoring and Review

Governors' Committee normally reviewing:	Governance
Effective from:	September 2025
Date of next review:	September 2026
Person responsible for implementation and monitoring	Bursar
Related policies and procedures:	• Privacy Notices • IT acceptable use • CCTV Policy • Cookie Policy