Data Protection

1 Introduction

1.1 The Heart of Mercia multi-academy trust (HoM) collects, uses, and stores Personal Data about its staff, suppliers, students, pupils, governors, directors, parents, and visitors. HoM recognises that having controls around the collection, use, retention, and destruction of Personal Data is important in order to comply with the Trust's obligations under Data Protection Laws. HoM's reputation is dependent on the way the organisation and all member academies manage and protect personal data. Protecting the confidentiality and integrity of personal data is a key responsibility of everyone within the organisation.

This policy has been prepared in accordance with the UK General Data Protection Regulation (UK) and the Data Protection Act 2018.

1.2 HoM is registered with the Information Commissioner's Office (ICO) as a data controller (registration number: ZA523083). The Data Protection Officer for HoM is contactable on dpo@heartofmercia.org.uk

2 Aims

2.1 The HoM aims to ensure that all personal data collected about its staff, suppliers, students, pupils, governors, directors, parents, visitors, and other individuals is collected, stored, and processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

3 Scope and Data Protection Principles

3.1 The UK GDPR and DPA 2018 set out the data protection principles that HoM must comply with. These principles say that personal data must be:

- process 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 purpose for which it is processed.
- accurate and, when necessary, kept up to date.
- kept for no longer than is necessary for the purpose for which it is processed.
- processed in a way that ensures it is appropriately secure.

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

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

4 Definitions

Definitions of the data protection terms used in the policy along with a brief explanation about what they mean can be found in Appendix 1.

5 Roles and Responsibilities

5.1 This policy applies to everyone who works for or with HoM, including external organisations or individuals working on our behalf. Staff, contractors, directors, governors, trustees, and anyone else that works with or on behalf of HoM must ensure that personal data is handled and processed in accordance with this policy and the data protection principles.

All HoM staff will be given comprehensive GDPR training before being allowed access to any personal data processed by the HoM.

New colleges and/or schools joining HoM Multi Academy Trust may continue to use their existing Data Protection Policy for a maximum of 12 months after their official joining date. The HoM DPO will review academy data protection policies during this period to ensure compliance with all statutory duties.

5.2 **Board of Trustees** – the Board of Trustees have overall responsibility for ensuring that HoM complies with relevant data protection publications.

5.3 **Data Protection Officer (DPO**) - the DPO is responsible for overseeing the implementation of this policy, monitoring compliance across HoM, and developing related policy and guidelines were applicable. They will work with the Data Protection Representatives in each member academy to ensure a consistent approach across all member academies.

The DPO will provide termly reports of data protection incidents across HoM to the Audit committee. They will also 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 HoM data protection issues.

The DPO is the point of contact for the supervisory authority (ICO) on issues relating to processing of personal data, and will consult with the supervisory authority, where necessary.

5.4 **Data Protection Representatives (DPR)** – each member academy has a DPR who is responsible for overseeing the implementation of this policy, monitoring compliance, and investigating data protection issues within their member academy. They are the first point of contact for all data protection matters within their academy including internal

reporting and record keeping. When necessary, the DPR will investigate any reportable breaches and report directly to the DPO. The DPR may be supported by relevant trained staff within the academy or across central services.

Academy DPRs can be contacted by email:

- dpo@hereford.ac.uk
- dpo@chantryschool.com
- dpo@jkhs.org.uk
- dpo@kedst.ac.uk
- dp.officer@wsfc.ac.uk

5.5 **The Chief Executive Officer**– the Chief Executive Officer acts as the representative of the data controller on a day-to-day basis.

5.6 **Staff** - all staff must comply with this policy and are responsible for:

- Collecting, storing, and processing any personal data in a secure manner and in accordance with this policy
- Informing their academy of any changes to their personal data, such as a change of address
- Contacting the DPR in the following circumstances:
  - if they have 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, draught privacy notice, deal with data protection rights invoked by an individual, full transfer personal data outside of HoM.
  - if there has been a data breach.
  - whenever they are engaging in a new processing activity that may affect the data privacy rights of individuals.
  - if they need help with contracts or sharing personal data with third parties.
- Not releasing or disclosing any personal data:
  - outside of their academy or HoM; or
  - inside the academy to persons not authorised to access the personal data without specific authorization from their DPR or the DPO.

6 Collecting Personal Data – Lawfulness Fairness and transparency

6.1 HoM will only process personal data where we have a legal basis (legal reason) to do so. The lawful bases are:

- The data needs to be processed so that the academy can **fulfil a contract** with the individual, or the individual has asked the academy to take specific steps before entering into a contract.
- The data needs to be processed so that the academy can **comply with a legal obligation.**
- The data needs to be processed to ensure the **vital interests** of the individual, e.g., to protect someone's life.
- The data needs to be processed so that the academy, as a public authority, can perform a task **in the public interest,** and carry out its official functions.
- The data needs to be processed for the **legitimate interests** of the academy 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 learner) has freely given **clear, explicit consent.**

HoM may also, for a specific purpose, collect and/or process special category personal data. This includes:

- personal data revealing **racial or ethnic origin**.
- personal data revealing **political opinions**.
- personal data revealing **religious or philosophical beliefs**.
- personal data revealing **trade union membership**.
- **genetic data**.
- **biometric data** (where used for identification purposes).
- data concerning **health**.
- data concerning a person's **sex life**; and
- data concerning a person's **sexual orientation**.

Special category personal data is more sensitive and requires greater protection. For special category personal data, the Trust recognises that, in addition to the legal bases (above), it must also meet one of the special category conditions for processing as set out in the UK GDPR and DPA 2018.

HoM will only collect and/or process special category personal data when necessary for a clearly identifiable purpose, and when there is no other reasonable or less intrusive way of achieving that purpose. The lawful bases on which HoM would process special category personal data can be found in UK GDPR, Article 9, Section 2. Details of these can be found at: https://ico.org.uk/fororganisations/guide-to-data-protection/guide-to-the-

general-data-protectionregulation-gdpr/lawful-basis-for-processing/special-category-data/

HoM will carefully assess both legal and illegal bases for collecting and processing all types of personal data when doing so, to ensure compliance with its duties and obligations under Data Protection legislation.

HOM will take necessary steps to ensure the protection of personal data whilst it is being processed. HoM will also ensure its destruction in line with the HoM Data Retention policy.

6.2 Where HoM collects personal data directly from individuals, we will inform them about how we are using their personal data in a privacy notice and the legal bases for doing so.

All member academies will have and make available the following privacy notices:

- Student/pupil privacy notice
- Student/pupil applicant privacy notice
- Staff/employee privacy notice
- Governor and trustee privacy notice
- Job applicant privacy notice
- Parent/guardian privacy notice

If HoM or any member academy changes how it uses personal data, the academy will update privacy notices, notify the individuals about the change, and seek consent where necessary. It is the responsibility of all members of staff to notify the Data Protection Representative in their academy if they intend to change how they use personal data.

7 Data Limitation, Minimisation and Accuracy

7.1 HoM recognises the importance of ensuring that personal data is limited, minimised, amended, rectified, erased or its use restricted where this is appropriate under data protection laws.

7.2 HoM will only collect personal data for specified explicit and legitimate reasons. The reason will be explained to the individual when we first collect their data (see section 6 above).

All HoM Staff that obtain personal data from sources outside their academy shall take reasonable steps to ensure that the personal data is recorded accurately, is up to date and limited to that which is adequate, relevant, and limited to what is necessary in relation to the purpose for which it is collected and used. This does not require academy or Trust personnel to independently check the personal data obtained.

7.3 All HoM staff that collect and record personal data shall ensure that the personal data is recorded accurately and kept up to date. HoM staff shall ensure that they limit the collection and recording of personal data to that which is accurate, relevant, and limited to what is necessary in relation to the purpose for which it is collected and used. HoM staff will only process and access data that is relevant to their jobs.

7.4 In order to maintain the quality of personal data, all HOM staff that access personal data shall ensure that they review, maintain, and update it to ensure that it remains accurate, up to date, adequate, relevant, and limited to what is necessary in relation to the purpose for which it is collected and used. Please note that this does not apply to personal data which the academy must keep in its original form (e.g., for legal reasons or that which is relevant to an investigation).

8 Data Retention

8.1 HoM will not keep personal data longer than is necessary for the purpose or purposes for which it is collected. Personal data will be retained in accordance with the HoM Data Retention Policy and HoM Data Retention Schedule. When relevant, data will be securely destroyed in accordance with the HoM Data Retention Policy.

9 Data Security

9.1 HoM will take measures to ensure the personal data they hold is kept safe from unauthorised or unlawful access, alternation, processing, or disclosure, against accidental or unlawful loss, destruction, or damage.

The measures HoM takes to ensure digital data security are outlined in the HoM Information Security Policy.

Personal data contained in physical paper records is subject to the following data security rules:

- Paper-based records 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, pinned to notice/display boards, or left anywhere else where there is general access.

10 Data Processing Partners

10.1 Staff should not share any personal information to third parties, without firstly discussing

with the Data Protection Representative at their member academy. This may include, but is not limited to, requests for references, examination results or confirmation that a learner is studying in any of our member academies.

HoM will not normally share personal data with anyone else, but may do so where:

- There is an issue with a learner or parent/carer that puts the safety of staff or learners at risk.
- We need to liaise with other agencies - we will seek consent as necessary before doing this.

HoM will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- the prevention of detection of crime and/or fraud
- the apprehension or prosecution of offenders
- emergency services and local authorities to help them respond to an emergency that affects any of our staff or learners.
- the assessment or collection of tax owed to HMRC.
- in connection with legal proceedings
- whether disclosure is required to satisfy our safeguarding obligations
- research and statistical purposes if personal data is sufficiently anonymised or consent has been provided.

10.2 HoM will sometimes appoint contractors and other service providers. This may require them to process some of the Trust's personal data on our behalf. HoM will carry out sufficient due diligence and have contracts in place to ensure necessary checks take place to protect any personal data that is shared outside of HoM. These checks will be undertaken before any personal data is shared. HoM will also undertake audits periodically to ensure that contractors are continuing to meet the required terms of their contract in relation to Data Protection.

GDPR requires the contract with a Processor to contain the following obligations as a minimum:

1. to only act on the written instructions of the Controller.
2. to not export personal data without the Controller's instruction.
3. to ensure staff are subject to confidentiality obligations.
4. to take appropriate security measures.
5. to only engage sub-processors with the prior consent (specific or general) of the Controller and under a written contract.
6. to keep the personal data secure and assist the Controller to do so.

7. to assist with the notification of Data Breaches and Data Protection Impact Assessments.
8. to assist with subject access/individual's rights.
9. to delete/return all personal data as requested at the end of the contract.
10. to submit to audits and provide information about the processing; and
11. to tell the Controller if any instruction is in breach of the GDPR or other Data protection law.

In addition, the contract should set out:

1. the subject matter and duration of the processing.
2. the nature and purpose of the processing
3. the type of personal data and categories of individuals; and
4. the obligations and rights of the controller

10.3 If HoM transfers personal data to a country or territory outside the European Economic Area, it will do so in accordance with Data Protection law. Data Subjects will be informed via relevant privacy notices.

11 Data Protection Impact Assessments

11.1 Data Protection Impact Assessments (DPIA) are carried out by HoM and its member academies to identify, analyse, and minimise risks arising out of processing personal data. DPIAs are carried out when HoM is launching or proposing to adopt a new process, product or service which involves personal data. HoM will consider whether it needs to carry out a DPIA as part of the initial project planning. DPIAs will be carried out at an early stage before any personal data is collected and/or processed.

HoM will use the ICOs (Information Commissioner's Office) guidance when completing DPIAs and assessing data protection risks.

DPIAs should be carried out by the project lead in consultation with Data Protection Representative or Data Protection Officer. The Data Protection Officer will review and approve all DPIAs and report to appropriate members of the Trust executive and /or academies.

12 The Rights of Data Subjects/individuals

12.1 Subject Access requests

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

- confirmation that their personal data is being processed.
- access to a copy of the data
- The purpose 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, and the criteria used to determine this period.
- The source of the data, if not the individual themselves
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

Subject access requests will be processed in accordance with the data protection law and advice on best practice from the Information Commissioner's Office (ICO).

If staff receive a subject access request, they must immediately forward it to the Data Protection Representative at their member academy.

12.1.2 Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or career 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 subject access request or have given their consent.

Children aged 12 and above are 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 learners over the age of 12 may not be granted without the express permission of the learner. However, this is not a rule and the learners' ability to understand their rights will always be judged on a case-by-case basis.

12.1.3 Separate to UK GDPR, parents of learners at our member academies are entitled to request access to or a copy of an annual written report of their son's or daughter's progress and attainment in the main subject areas taught, in accordance with Education (Independent School Standards) Regulations 2014. Requests for further information will be processed as a subject access request.

12.1.4 When responding to subject access requests, the Trust:

- may require the individual to provide two forms of identification.
- may contact the individual via phone to confirm the request was made.
- will respond without delay from within the time limit set by the ICO.
- will normally provide 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 numerous. We will inform the individual of this within 1 month and explain why the extension is necessary.

12.1.5 If a subject access request is refused, the Trust will inform the individual of the reasons for the refusal.

If a request is unfounded or excessive, we may refuse to act on it or charge a reasonable fee which takes into account administrative costs.

12.1.6 If an individual receives a response to a subject access request from HoM, but is unhappy for any reason, they should first make a complaint to HoM using the HoM Complaints policy.

12.1.7 If an individual has complained to HoM and has not received any response or remains unhappy with the Trusts handling of their subject access request, they can make a complaint to the ICO. Details of how to do this and the role of the ICO in such circumstances can be found here What to do if the organisation does not respond or you are dissatisfied with the outcome | ICO

12.2 Right to be forgotten (erasure)

There is a limited right for individuals to request the erasure of personal data concerning them where:

- the use of the personal data is no longer necessary.
- their consent is withdrawn and there is no other legal ground for the processing.
- the individual objects to the processing and there are no overriding legitimate grounds for the processing.
- The personal data has been unlawfully processed; and the personal data must be erased for compliance with a legal obligation.

Individuals should submit any request to exercise this right to the Data Protection Representative at their member academy.

12.3 Right of data portability

An individual has the right to request that data concerning them is provided to them in a structured, commonly used, and machine-readable format where the processing is based on consent or on a contract; and the processing is carried out by automated means.

This right is different from subject access and is intended to give individuals a subset of their data.

Individuals should submit any request to exercise this right to the Data Protection

Representative at their member academy.

12.4 Right of Rectification and Restriction

Individuals are also given the right to request that any personal data is rectified if inaccurate and to have the use of their personal data restricted to particular purposes in certain circumstances.

Individuals should submit any request to exercise this right to the Data Protection

Representative at their member academy.

12.5 Other Data Protection rights of the individual

HoM will use all personal data in accordance with the rights given to individuals' and will ensure that it allows individuals to exercise their rights in accordance with Data Protection laws.

Individuals also have the right to:

- the right to be informed of any changes to the processing of their data (see section 6)
- the right to restrict processing (see section 6)
- the right to object to the processing of their data (see section 6)
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, which might negatively affect them)
- Be notified of a data breach in certain circumstances.
- Make a complaint to the ICO.

13 CCTV

We use CCTV in various locations around all our academy sites to ensure they remain safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear on-site that individuals are being recorded. Security cameras are clearly visible and there is signage explaining that CCTV is in use.

Each member academy has a separate CCTV policy that is available on request.

Any enquiries about the CCTV system should be directed to the Estates or Business Manager at each academy.

14 Photographs and Videos

Our member academies may take photographs and record images of individuals within our schools and colleges.

Each member academy will communicate to individuals featured in the photograph or recording and individuals will have the right to object to their image being used. Consent for the use of the images will be taken from the individuals or an appropriate adult in the case of younger learners. The consent will clearly state the intended use of the images.

Consent can be refused or withdrawn at any time by contacting the Data Protection Representative at the member academy. If consent is withdrawn the member academy will delete the photograph or video and not distribute it further.

15 Data Breaches

HoM takes data protection and information security very seriously and will take all reasonable measures to ensure that there are no personal data breaches. However, unfortunately, it is still possible for data breaches to occur.

In the event of a suspected data breach, we will follow set procedures. These procedures are set out in Appendix 2.

Examples of data breaches may include, but are not limited to:

- Confidentiality breach – where there is an unauthorised or accidental disclosure of, or access to, personal data. This could be through a direct action or inaction, hacking, accessing internal systems that they are not authorised to access, accessing personal data stored on a lost laptop, phone, or other device, placing personal data in the public forum or where it can be invertedly seen, sending an email to the wrong learner or disclosing information over the phone to the wrong person.
- Availability breach – where there is an accidental or unauthorised loss of access to, or destruction of, personal data, e.g., A denial of service attack, infection of systems by ransomware, deleting personal data in error, loss of access to personal data stored on systems, inability to restore access to personal data from, loss of an encryption key.
- Integrity breach – where there is an unauthorised or accidental alteration of personal data.

16 Training

All staff, governors and volunteers will receive data protection training as part of their induction process. In addition, staff will receive annual data protection refresher training, delivered within their member academy.

Briefings (meetings or electronic) may be used to update staff on data protection issues where necessary.

Further data protection will form part of continuing professional development, where changes to legislation, guidance or the college's processes make it necessary.

17 Data Protection by Design and Default

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

- appointing a suitably qualified DPO and ensuring that they have the necessary resources to fulfil their duties and maintain their expert knowledge.
- only process personal data that is necessary for each specific purpose for processing, and always in line with the data protection principles set out in relevant data protection law.
- integrating data protection into internal documents including this policy, any related policies and privacy notices
- regularly train 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 it of attendance at data protection training sessions.
- regularly conduct reviews and audits to test our data protection measures and make sure we are compliant.
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, we can make available the information we are required to share about how we use and process personal data.
    - For all personal data we hold, maintaining a record of the type of data, data subjects, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data safe.

18 Link policies

This data protection policy is linked to our:

- Biometric Information Policy at relevant member academies
- CCTV Policy at each member academy.
- Digital Images Policy at selected academies.
- HoM Access to Information Policy (including the publication scheme)
- HoM Data Retention Policy
- HoM Information Security Policy.

- HoM Whistleblowing Policy.
- Privacy Policies at each member academy.
- Staff Acceptable Use Policy at each member academy.
- Staff Code of Conduct at each member academy.
- Staff Wellbeing Policy at each member academy.
- Learner Acceptable Use Policy at each member academy.

19 Equality Impact

The Trust's responsibilities towards promoting equality, diversity and inclusion have been considered when drafting this policy.

20 Review

This policy will be reviewed annually; if new data protection legislation or guidance is issued; or when new academies join HoM.

Date of review	Date agreed	MAT Board	LGBs	Review date	Comments
14/10/24	12/12/2024	12/12/2024	Spring 2025	10/25	

Appendix 1: Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, 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 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.

Appendix 2: Data Security and Data Protection Incident Management

Procedure for discovering and reporting data breaches.

This procedure is based on guidance on personal data breaches produced by the ICO. All HOM staff are expected to follow these procedures so HOM can ensure a structured and effective response to a data breach, minimising its impact and helping to protect sensitive information.

1. Immediate Response

- **Identify the Breach**: As soon staff or anyone working for or on behalf of HOM suspects or identifies a data breach, they must immediately report the breach to the Data Protection Representative (DPR).
    - If the breach involves electronic data, they must immediately report to the IT team within the academy.
- **Contain the Breach**: Relevant staff must take immediate steps to contain the breach. This may involve isolating affected systems, changing passwords, or disabling accounts. The IT team and DPR in the academy can advise on the best steps to take.

2. Assessment

- **Assess the Impact**: The DPR should determine the type of data involved, the extent of the breach, and the potential impact on individuals and the organisation.
    - The DPR will report the breach on our reporting software.
    - In academies that have self-reporting functionality active, staff discovering the breach should report the breach on our reporting software.
- **Gather Evidence**: The DPR should, with the help of the person/organisation who discovered the breach, collect, and preserve evidence related to the breach for further investigation and legal purposes.

3. Notification

- **Inform the Data Protection Officer (DPO) and management**: Notify the DPO and senior management at the academy and relevant stakeholders about the breach.
- **Report to Authorities**: If required, the DPO will report the breach to the Information Commissioner's Office (ICO) within 72 hours of discovery.
- **Notify Affected Individuals**: Inform individuals whose data has been compromised, providing them with details of the breach and steps they can take to protect themselves.

4. Investigation

- **Conduct a Thorough Investigation**: The DPR, with help from other relevant staff, should investigate the cause of the breach, how it occurred, and the extent of the damage.
- **Engage Experts**: If necessary, engage the HOM cybersecurity expert, or other experts to assist with the investigation and remediation efforts.

5. Remediation

- **Fix Vulnerabilities**: Address and fix any vulnerabilities that led to the breach to prevent future occurrences.
- **Review Policies and Procedures**: Review and update data protection policies and procedures based on the findings of the investigation.

6. Documentation and Reporting

- **Document the Incident**: Update the breach reporting software of the response actions taken, and the outcomes of the investigation.

7. Follow-Up

- **Monitor Systems**: Continuously monitor systems for any signs of further breaches or vulnerabilities.
- **Provide Training**: Offer additional training to employees on data protection and breach response procedures.