Diocese of Hereford Multi-Academy Trust

Data Protection Policy

Review: Sept 2027

Contents

1. Aims

1.1 We aim to ensure that all data collected regarding staff, pupils, parents, and visitors is collected, stored, and processed, in accordance with UK data protection law.

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

2. Legislation and guidance

2.1 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.

2.2 Data Protection Act 2018

2.3 Data (Use and Access) Act 2025

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

2.5 It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

2.6 It also reflects the ICO's guidance for the use of surveillance cameras and personal information.

2.4 This policy complies with our Funding Agreements and Articles of Association as a member of The Diocese of Hereford Multi-Academy Trust (DHMAT)

3. Definitions

Term	Definition
Personal data	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified
Sensitive personal data	Data such as: Contact details Racial or ethnic origin Political opinions Religious beliefs, or beliefs of a similar nature Where a person is a member of a trade union Physical and mental health

	Sexual orientation Whether a person has committed, or is alleged to have committed, an offence Criminal convictions
Processing	Any activity that involves the use of personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual and also includes transmitting or transferring personal data to third parties.
Data Subject	The person whose personal data is held or processed
Data Controller	A person or organisation that determines the purposes for which, and the manner in which, personal data is processed
Data Processor	A person, other than an employee of the data controller, who processes the data on behalf of the data controller
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The Data Protection Officer

4.1 As a Trust, we are required to appoint a Data Protection Officer (DPO). Our DPO is HY Education.

T: 0161 543 8884.

Email: dpo@wearehy.com

4.2 The Trust's Chief Finance Officer is the Trust's DPO Lead – contact details:

Greg Evans – Head of Finance & Resources

g.evans@dhmat.org.uk

5. The Data Controller

5.1 The school is a part of the Diocese of Hereford Multi-Academy Trust, who processes personal information relating to pupils, staff, and visitors, and, therefore, are the Data Controller.

5.2 The Trust is registered as a Data Controller with the Information Commissioner's Office.

6. Data Protection principles

6.1 The UK GDPR is based on the following data protection principles:

- Data shall be processed fairly and lawfully and in a transparent manner
- Personal data shall be obtained only for specified, explicit and legitimate purposes
- Personal data shall be relevant and not excessive in relation to the purpose(s) for which it is processed
- Personal data shall be accurate and, where necessary, kept up to date
- Personal data shall not be kept for longer than is necessary for the purpose(s) for which it is processed
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of, or damage to personal data
- Appropriate measures in place to ensure compliance with data processing principles.

7. Roles and responsibilities – Trust staff are responsible for:

7.1 Collecting, storing and processing any personal data in accordance with this policy.

7.2 Informing the Trust of any changes to their personal data, such as change of address or name.

7.3 Contacting the DPO or DPO lead 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 or not they have a lawful basis to use personal data in a particular way
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals

- If they need help with any contracts or sharing personal data with third parties

8. Collecting personal data

8.1 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:

I. The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract

II. The data needs to be processed so that the school can **comply with a legal obligation**

III. The data needs to be processed to ensure the **vital interests** of the individual or another person i.e. to protect someone's life

IV. The data needs to be processed so that the school, as a public authority, can **perform a task in the public interest or exercise its official authority**

V. The data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the school performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden

VI. 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.

8.2 Limitation, minimisation and accuracy

We will only collect personal data for specified explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

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

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

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

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule.

9. Sharing personal data

Generally, we are not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

There will be certain circumstances where we may be required to share personal data. These include, but are not limited to, situations where:

- There is an issue with a pupil, or a parent or 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.

10. Subject access requests (SARs)

10.1 Subject access requests (SARs)

By law, individuals have a right to make a 'subject access request' (SAR) to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for or, if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not the individual

- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally
- Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:
- The 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.

10.1 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.

FOR PRIMARY SCHOOLS

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

FOR SECONDARY SCHOOLS

10.3 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 numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary (these timeframes continue to apply when the school is closed during holidays)

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 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.

10.4 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 8), individuals also have the right to:

- Withdraw their consent to processing at any time
- Receive certain information about the data controller's processing activities
- 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 personal 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.

11. 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. Measures we take include:

- Paper-based records that contain sensitive information are kept under lock and key when not in use
- Papers containing confidential personal information should not be left on office tables or pinned to noticeboards where there is general access
- Where personal information needs to be taken off-site (in paper or electronic form), staff must ensure it is secure and in their possession at all times
- The Headteacher may authorise staff to use school laptops off site.
- Passwords containing letters and numbers are used to access computers, laptops, and other electronic devices. Staff are reminded to follow the guidance from their ICT support regarding password management

- Storage of personal information on personal devices should be avoided. Should there be an unavoidable need to store personal information on personal devices all Staff, pupils, or LGB members must follow the same security procedures for -owned equipment.

12. Artificial Intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini. DHMAT 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.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, DHMAT will treat this as a data breach.

13. Photographs and videos

- As part of our school activities, we may take photographs and record images of individuals within our school.
- For primary schools we will obtain written consent from parents and 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 parents/carers and the pupil.

- Any photographs and videos taken by parents and carers at school events for their own personal use are not covered by data protection legislation. However, if photos or videos are allowed, 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.
- For secondary schools, we will obtain written consent from parents and carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.
- Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parents/carers and the pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.
- Any photographs and videos taken by parents and carers at school events for their own personal use are not covered by data protection legislation. However, if these are allowed, 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 (or pupils where appropriate) have agreed to this.

- Where the school takes photographs and videos, uses may include:
  - Within school on notice boards and in school brochures, newsletters, etc.
  - Outside of school by external agencies such as the school photographer, newspapers, campaigns
  - Online on our school 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.

14. Biometric data & CCTV

- Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use fingerprints to take payment for school dinners instead of cash, we will comply with the requirements of the Protection of Freedoms Act 2012 and the UK GDPR.
- Parents and carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least 1 parent or carer before we take any biometric data from their child and first process it.

- Parents and carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners in cash at each transaction if they wish.
- Parents and carers and pupils can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.
- As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).
- Where staff members or other adults use the school's biometric system(s), we will also obtain their explicit consent before they first take part in it and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.
- We use CCTV in various locations around the school 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.

15. Disposal of records

Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely. For example, we will shred or incinerate paper-based records and override electronic files. We may also use an outside company to safely dispose of electronic records.

16. Training

14.1 Our staff and Local Governing Board members are provided with data protection training as part of their induction process.

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

14.3 Staff will undertake annual NCSC cyber-training

17. Complaints

We take any complaints about how we collect and use personal information very seriously. If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concerns about our data processing, please raise this with us in the first instance. You can make a complaint to us at any time by contacting our DPO.

Upon receiving a complaint, we will:

- Acknowledge receipt of the complaint within 30 days of receiving it
- Without undue delay, take appropriate steps to respond to the complaint, including:
    - Making appropriate enquiries based on the circumstances of the complaint
    - Keeping the complainant informed on the progress of the investigation
    - Without undue delay, inform the complainant of the outcome of the investigation

18. Monitoring arrangements

The DPO Lead is responsible for monitoring and reviewing this policy

This policy will be reviewed annually and approved by Board

19. Links with other policies and documents

Freedom of information Policy

Privacy Notices

Appendix 1

Diocese of Hereford Multi-Academy Trust

Procedures for responding to Subject Access Requests made under Data Protection Act 2018 and General Data Protection Regulations

Rights of access to information

Under the Data Protection Act 2018 and GDPR, any individual has the right to make a request to access the personal information held on them.

Actioning a Subject Access Request

1. Request for information must be made in writing, and we have provided a form for this purpose:
2. The identity of the requestor must be established before the disclosure of any information, and checks will be carried out regarding proof of relationship to the child if a parent is making a request. Evidence of identity can be established by combination of the following documents:
    a. Passport
    b. Driving licence
    c. Utility bills with current address
    d. Birth/marriage certificate
    e. P46/P60
    f. Credit card or mortgage statement
3. Any individual has the right of access to information held about themselves. However, with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. Personal data about a child belongs to that child. The Trust will decide on a case-by-case basis whether to grant such request, bearing in mind guidance issues from time to time from the Information Commissioner's Office.
4. The deadline to respond to a subject access request is one month. However, the one month will not commence until after clarification of the information sought. Response to a SAR can be extended by up to 2 additional months if the request is complex or in the event of multiple requests.
5. The Data Protection Act 2018 allows exemptions regarding the provision of some information: therefore, all information will be reviewed prior to disclosure.
6. Third party information is that which another body, such as the Police, Local Authority, Health Care professional or another school, has provided. Before disclosing third party information consent will normally be obtained. Statutory timescales will still apply.

7. Any information, which may cause serious harm to the physical or mental health or, emotional condition of the pupil or another individual may not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings be disclosed.
8. If there are concerns over the disclosure of information, then additional advice should be sought.
9. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.
10. Information disclosed should be clear, thus, any codes or technical terms would need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.
11. Information can be provided at the school with a member of staff on hand to help and explain matters if requested. The view of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used, then registered/recorded mail must be used.

Safeguarding

DHMAT's responsibilities in relation to Child Protection and Safeguarding will always be considered and where there is any doubt about whether or not to disclose information then Safeguarding priorities will take precedence over Data Protection and Subject Access Requests.

Complaints

Complaints about the above procedures should be referred to DHMAT's Chief Finance Officer who will decide whether it is appropriate for the complaint to dealt with in accordance with the Data Protection Complaints Policy. The Information Commissioner can deal with complaints, which are considered to be outside the scope of DHMAT's Complaints Policy. Contact details of both will be provided with the disclosure information.

Contacts

If you have any queries or concerns regarding this procedure, then please contact the Data Protection Officer. Contact details are available on request.

Diocese of Hereford Multi-Academy Trust

SUBJECT ACCESS REQUEST FORM

Please complete this form if you want us to supply you with a copy of any personal details, we hold about you.

We will endeavour to respond promptly and in any event within one month of the latest of the following:

- Our receipt of your written request; or
- Our receipt of any further information we may ask you to provide to enable use to comply with our request.

The information you supply in this form will only be used for the purposes of identifying the personal data you are requesting and responding to our request. You are not obliged to complete this form to make a request but doing so will make it easier for us to process your request quickly.

1) Details of the person requesting information

Full Name:

Address (including postcode):

Contact Telephone Number:

Contact Email Address:

To ensure we are releasing data to the right person we require you to provide us with proof of your identity and of your address. If we are not satisfied you are who you claim to be, we reserve the right to refuse to grant your request.

Please supply us with a photocopy or scan image (do not send the originals) of one of **both** of the following:

a) Proof of Identity: Passport, photo driving licence, national identity card, birth certificate.
b) Proof of Address: Utility bill, bank statement, credit card statement (no more than 3 months old); current driving licence; current TV licence: Local Authority tax bill, HMRC tax document (no more than 1-year-old). Alternatively, you can post this proof of identification to DHMAT.

2) What information are you seeking?

Please describe the information you are seeking. Please provide any relevant details you think will help us to identify the information you require. Please note that if the information you request reveals details directly or indirectly about another person, we will have to seek the consent of that person before we can let you see that information. In certain circumstances, where disclosure would adversely affect the rights and freedoms of others, we may not be able to disclose the information to you, in which case you will be informed promptly and given full reasons for that decision. While in most cases we will be happy to provide you with copies of the information you request, we nevertheless reserve the right, in accordance with article 12 of the GDPR to charge a fee or refuse the request, if it is considered to be "manifestly unfounded or excessive". However, we will make every effort to provide you with a satisfactory form of access or summary of information whichever is suitable.

3) Details of the person requesting information

If you want information about any of the following, please tick the boxes:

☐ Why we are processing your personal data

☐ To whom your personal data is disclosed

☐ The source of your personal data

4) Declaration

I confirm that I have read and understood the terms of this subject access form and certify that the information given in this application is true. I understand that it is necessary for DHMAT to verify my identity and it may be necessary to obtain more detailed information in order to locate the correct personal data.

Signed: Date:

Appendix 2

Diocese of Hereford Multi-Academy Trust

Data Breach Procedure

This procedure is designed to ensure that all staff, LGB members, and Directors are aware of what to do in the event of a DPA/GDPR breach and that they need to act swiftly to report the breach.

DHMAT recognises that most breaches, aside from cyber-criminal attacks, occur as a result of human error. They are not malicious in origin and if quickly reported are often manageable.

Examples of breaches are:

- Information being posted to an incorrect address which results in an unintended recipient reading that information
- Loss of mobile or possible data devices, unencrypted mobile phones, laptops, USB memory sticks or similar
- Sending an email with personal data to the wrong person or too many people who may not need to or be entitled to see the data
- Dropping or leaving documents containing personal information in a public place
- Personal data being left unattended at a printer enabling unauthorised personnel to read that information
- Not securing documents containing personal data (at home or work) when left unattended
- Anything that enables an unauthorised individual access to school buildings or computer systems
- Discussing personal data with someone not entitled to it, either on the phone or in person. How can you be sure they are entitled to that information?
- Deliberately accessing or attempting to access or use personal data beyond the requirements of an individual's job role e.g. for personal, commercial, or political use. This action may constitute a criminal offence under the Computer Misuse Act as well as the Data Protection Act.
- Opening a malicious email attachment or clicking on a link from external or unfamiliar sources, which leads to DHMAT's equipment (and subsequently its records) being subjected to a virus or malicious attack, which results in unauthorised access to, loss, destruction or damage to personal data.

What should staff do?

Being open about the possible breach and explaining what has been lost or potentially accessed is an important element of working with the ICO to mitigate the impact. Covering up a breach is never acceptable and may be a criminal, civil or disciplinary matter. Report the breach to the Headteacher and Data Protection Officer as soon as possible, this is essential.

What will happen next?

The breach notification form will be completed and the breach register updated. Where relevant, the breach report to the ICO will be submitted within 72 hours of the Data Protection Officer becoming aware of the breach.

If the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data, breach notification to those people will be done in a co-ordinated manner with the support from the ICO.

Breach notification to data subject

For every breach, DHMAT will consider notification to the data subject or subjects as part of the process. If the breach is likely to be high risk, they will be notified as soon as possible and kept informed of any actions and outcomes.

The breach and process will be described in clear and plain language.

If the breach affects a high volume of data subjects or and personal data records, the most effective form of notification will be used and discussed with the Head teacher with support from the Data Protection Officer.

Advice will be taken from the ICO about how to manage communication with data subjects if appropriate.

A post breach action plan will be put in place and reviewed.

Evidence collection

It may be necessary to collect information about how information security breach or unauthorised release of data occurred. This evidence gathering process may be used as part of an internal process (which can include disciplinary procedures), it may be a source of information for the ICO, and it could be used within criminal or civil proceedings

This process will be conducted by a suitable member DHMAT, which may or may not be the Data Protection Officer but will be determined the best way to secure evidence.

Guidance may be required from an external legal provider, and the police may be involved to determine the best way to secure evidence.

A record of what evidence has been gathered, stored, and secured must be available as a separate log. Files and hardware must be securely stored.

Evidence Collection Log

Date	Evidence Description	Secure storage location & confirmed data	Trust Officer

Data Breach Notification Form

When did the breach occur (or become known)?	
Who was involved in DHMAT?	
Who was this reported to?	
Date and time, it was reported	
Date and time DPO notified	
A description of the nature of the breach. This must include the type of information that was lost, e.g. name, address, medical information, NI number	
The categories of personal data affected – electronic, hard copy	
Approximate number of data subjects affected	
Approximate number of personal data records affected	
Name and contract details of the Data Protection Officer/GDPR Owner	
Consequences of the breach. What are the potential risks?	
Any measures taken to address the breach. What actions and timeline have been identified?	
Any information relating to the data breach.	