Diocese of Hereford Multi-Academy Trust

Data Protection Policy

Approved	Dec 2021
Review	Sept 2024
Version	3.3

Contents

The Diocese of Hereford Multi-Academy Trust (Trust) are the Data Controller for the purposes of the Data Protection Act (DPA) 1998 and the General Data Protection Regulations 2018.

The DPA defines “Personal Data” as data that relates to a living individual who can be identified: -

- from that data, or
- from that data and other information, which is in the possession of, or is likely to come into the possession of, the Data Controller.

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 the Data Protection Act 1998, and the General Data Protection Regulations 2018.

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

2. Legislation and guidance

2.1 This policy meets the requirements of the UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020 and Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the information commissioner's office (ICO) on the UK GDPR.

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

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

2.4 In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

2.5 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	Obtaining, recording, or holding data
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 based at the Central Office and contact details are as follows: -

Mr Greg Evans

Chief Finance Officer

Diocese of Hereford Multi-Academy Trust,

Unit 11, The Business Quarter, Ludlow Eco Park,

Sheet Road,

Ludlow,

Shropshire,

SY8 1FD.

T: 01584 838 880

E: dpo@dhmat.org.uk

4.2 The DPO is responsible for ensuring compliance with the Data Protection legislation and with this policy. Any questions about the operation of the policy, or any concerns that the policy has not been followed, should be referred, in the first instance, to the School Protection Officer (SPO).

4.3 The DPO is also the central point of contact for all **data subjects** and others in relation to matters of data protection.

5. The Data Controller

5.1 The academy 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 Data Protection Act 1998 and the General Data Protection Regulations 2018 are based on the following data protection principles, or rules for good data handling:

- Data shall be processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful 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
- Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998
- 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
- Personal data shall not be transferred to a country or territory outside the European Economic Area, unless the country or territory ensures an adequate level of protection for the rights and freedoms of data, in relation to the processing of personal data

7. Roles and responsibilities

7.1 This policy applies to **all staff** employed by the Trust, who has overall responsibility for ensuring that the Trust complies with its obligations under the Data Protection Act 1998 and the General Data Protection Regulations 2018.

7.2 Data protection is the responsibility of the CEO, and day-to-day responsibilities rest with the Headteachers, in each of the academies.

7.3 The Headteacher will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data. The Headteacher may delegate some duties to a designated member of staff but retains the overall responsibility for the academy.

7.4 Staff are responsible for ensuring that they collect and store any personal data in accordance with this policy. Staff must also inform the academy of any changes to their personal data, such as a change of address.

8. Privacy/Fair Processing notice

8.1 Pupils and parents

We hold personal data about pupils to support teaching and learning, to provide pastoral care and to assess how the academy is performing. We may also receive data about pupils from other organisations including, but not limited to, other academies, Local Authorities, and the Department for Education.

This data includes, but is not restricted to:

- Contact details
- Results of internal assessment and externally set tests
- Data on pupil characteristics, such as ethnic group or special educational needs
- Exclusion information
- Details of any medical conditions

8.2 We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about pupils with anyone without consent, unless the law and our policies allow us to do so. Individuals who wish to receive a copy of the information that we hold about them/their child, should refer to sections 8 and 9 of this policy.

For secondary academies only

8.2.1 Once our pupils reach the age of 13, we are legally required to pass on certain information to our Local Education Authority, which has responsibilities in relation to the education or training of 13-19-year-olds. Parents, or pupils, if aged 16 or over, can request that only their name, address and date of birth be passed to the Local Authority by informing the Head teacher/designated member of staff.

8.2.2 We are required, by law, to pass certain information about pupils to specified external bodies, such as the Trust, Local Authority and the Department for Education, so that they are able to meet their statutory obligations.

8.3 **Staff**

We process data relating to those we employ to work at, or otherwise engage to work at, the academy. The purpose of processing this data is to assist in the running of the academy, including:

- Enable individuals to be paid
- Facilitate safe recruitment
- Support the effective performance management of staff
- Improve the management of workforce data across the sector
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring

8.4 Staff personal data includes, but is not limited to, information such as:

- Contact details
- National Insurance numbers
- Salary information
- Qualifications
- Absence data
- Personal characteristics, including ethnic groups
- Medical information
- Outcomes of any disciplinary procedure

8.5 *The Diocese of Hereford Multi-Academy Trust (Trust):* the employers for purposes of payroll and personnel information. We are required to share information about our employees with the DfE under section 5 of the Education (Supply of Information about the Academy Workforce) (England) Regulations 2007 and amendments. Payroll & personnel details are also shared with our payroll & HR provider (currently Shropshire County Council (Inspire to Learn) and the relevant pension funds.

8.6 *Local authority (LA):* We are required to share information about our workforce members with our LA under section 5 of the Education (Supply of Information about the Academy Workforce) (England) Regulations 2007 and amendments.

8.7 *Department for Education (DfE):* We share personal data with the DfE on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to academy funding / expenditure and the assessment educational attainment.

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

8.8 We will not share information about staff with third parties without consent unless the law allows us to.

8.9 We are required, by law, to pass certain information about staff to specified external bodies, such as our local authority and the Department for Education, so that they are able to meet their statutory obligations.

8.10 Any staff member wishing to see a copy of information about them that the academy holds should contact the Head teacher/designated member of staff.

9. Subject access requests (SARs)

9.1 Under the Data Protection Act 1998, and The General Data Protection Regulations 2018, pupils, staff, parents & carers have a right to request access to information the Trust holds about them, this is known as a Subject Access Request. Subject Access Requests must be submitted in writing, using the form available on the website www.dhmat.org.uk

9.2 The Trust will not reveal the following information in response to subject access requests:

9.2.1 Information that might cause serious harm to the physical or mental health of the pupil or another individual.

9.2.2 Information that would reveal that a pupil/staff is at risk of abuse, where disclosure of that information would not be in their best interests

9.2.3 Information contained in adoption and parental order records

9.2.4 Certain information given to a court in proceedings concerning the pupil/staff member

9.3 Subject Access Requests will usually be provided within one month. Current pupil educational records will be provided within 14 days.

10. Parental requests to view educational records

10.1 Personal data about a child belongs to that child, and not the child's parents. This is the case even where a child is too young to understand the implications of Subject Access Request rights.

10.2 For a parent to make a SAR, the child must either be unable to understand their rights and the implications of a request or have given their consent.

10.3 The Information Commissioner's Office (ICO), the organisation that uphold information rights, generally regards children aged 12 and above as mature enough to understand their rights and the implications of a subject access request. Therefore, most SARs from parents of pupils at our academies may not be granted, without the express permission of the pupil.

10.4 Parents of pupils at our academies do not have an automatic right to access their child's educational record. The academy will decide on a case-by-case basis whether to grant such requests, and we will bear in mind guidance issued from time to time from the Information Commissioner's Office. Requests will normally be provided within one month.

11. Storage of records

11.1 Paper-based records that contain sensitive information are kept under lock and key when not in use

11.2 Papers containing confidential personal information should not be left on office tables or pinned to noticeboards where there is general access

11.3 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

11.4 The Headteacher may authorise staff to use school laptops off site.

11.5 Passwords containing letters and numbers are used to access computers, laptops, and other electronic devices. Staff are reminded to change their passwords at regular intervals

11.6 Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.

11.7 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 LAB members must follow the same security procedures for academy-owned equipment.

12. Biometric data & CCTV

12.1 Biometric data is considered special category data and refers to the personal data about an individual's physical or behavioural characteristics and can be used to identify them, such as fingerprints or facial images. This data is collected and used as part of an automated biometric recognition system which measures these characteristics to identify an individual.

12.2 An automated biometric recognition system processes data when:

Recording pupil's biometric data e.g. measuring fingerprints via a scanner.

Storing biometric data on a database

12.3 Using biometric data as part of an electronic process e.g. by comparing it with data stored on a database to identify or recognise pupils.

12.4 Academies using biometric data must comply with the requirements of Protection of Freedoms Act 2012, and ensure the data is obtained, used and stored in accordance with GDPR regulations.

12.5 We use CCTV in various locations around school sites to ensure safety. We follow the ICO guidance for the use of CCTV and comply with data protection principles.

12.6 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.

Obtaining Consent

12.5 A school cannot lawfully process a pupil's biometric information without having obtained explicit consent.

12.6 Notifications sent to parents should include information about the processing of their child's biometric information that is sufficient to ensure that parents are fully informed about what is being proposed. It should include:

- Details of the type of data required
- How the data will be used
- The parents and pupils right to refuse or withdraw consent

- The Academy's duty to provide alternative arrangements for those whose information cannot be processed.

12.7 Unambiguous consent must always be used for biometric data usage – it must be freely given, specific and informed, and obtained on an opt-in basis. All parents of pupils under the age of 16 must be notified for consent if the academy wishes to take and use their child's biometric data as part of an automated biometric recognition system.

12.8 Academy's will not be required to obtain consent for biometric information from a particular parent if any of the following applies:

- The parent cannot be found, e.g. their whereabouts or identify are not known
- The parent lacks the mental capacity to provide consent or object to processing
- The welfare of the pupil requires that a particular parent is not contacted
- It is otherwise not reasonably practicable for a particular parent to be notified or their consent to be obtained.

12.9 If neither parent can be notified for any of the above reasons, section 27 of the protection of freedoms act 2012 explains that, if a child is being looked after by an LA or voluntary organisation, it is they who must be notified and have their written consent approved. If this does not apply, those caring for the child must be notified and written consent must be obtained from at least one carer.

The Right to object/withdraw

12.10 Providing the pupil or parent does not object, the school will only need the written consent of one parent in order to process biometric data.

12.11 A pupil's objection overrides any parental consent to the processing; if a pupil under 16 refuses to participate, the school must ensure the pupil's biometric data is not taken or used as part of a biometric recognition system. If consent is withdrawn, the school must ensure that any relevant data that has been captured is deleted.

12.12 Academies should ensure pupils understand their right to object or refuse their biometric data to be taken, or used. The academy should also inform parents of their child's right to object, and ensure the steps they take to inform pupils to take account of their age and level of understanding.

Reasonable Alternatives

12.13 Should a pupil or their parent object to having their biometric data taken and used, the academy must provide them with an alternative method of accessing relevant services.

12.14 Pupils should not suffer any disadvantage or difficulty in accessing services or premises due to not participating in an automated biometric recognition system, and such alternative arrangements should not place any additional burden on parents/carers whose children are not participating.

13. Disposal of records

13.1 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.

14. Training

14.1 Our staff and LAB 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 academy's processes make it necessary.

All staff are expected to adhere to these guidelines:

Always use a strong password, containing alpha/numeric combinations

Encrypt emails containing data or share via 'OneDrive'

Lock your computer before leaving your workspace

Make sure your anti-virus software is up to date

Ensure security of unprotected data taken out of office/academy

Only use encrypted memory cards and USB drives

Paper-based data - COVER IT! LOCK IT! SHRED IT!

15. Withdrawing consent

15.1 Consent can be withdrawn subject to contractual, statutory, or regulatory constraints. Where more than one person has the ability to provide or withdraw consent the Trust will consider each situation on its merits and within the principles of GDPR and child welfare, protection, and safeguarding principles. We have provided a form for you to withdraw consent and this is in Appendix 1

16. Complaints

16.1 If you have a concern about how your data has been collected, used, held, or processed by the Trust, then please refer to the Complaints Procedure in the first instance, which is available on our website. You have a right to complain if you feel that data has been shared without consent or lawful authority, or if you have asked us to erase, rectify, not process data and we have not agreed to your request. We will seek to resolve issues on an informal basis and then through our formal complaint's procedure.

16.2 In the UK, it is the ICO who has responsibility for enforcing the GDPR obligations and their contact details can be found at https://ico.org.uk/ Helpline 0303 123 1113 Email: casework@ico.org.uk

17. Monitoring arrangements

17.1 The Directors and CEO are responsible for monitoring and reviewing this policy. At every review, the policy will be shared with the full Board of Directors. Monitoring is also undertaken by the Trust's Data Protection Officer.

17.2 The Headteacher alongside the Local Academy Board checks that the academy complies with this policy by, among other things, reviewing academy records termly.

17.3 This document will be reviewed every two years.

18. Links with other policies and documents

Freedom of information Policy https://ico.org.uk

Information Management for Academy – IRMS Academies Toolkit - Information and Records Management Society

Retention of Documents

Privacy Notice – Staff

Privacy Notice – Pupils

Updates	Date:
Details of Data Protection Officer included	March 2019
Rebrand trust name change and reformat, no content change	September 2019
Update to include section on Withdrawing Consent; Complaints; Biometric Data and the appendices; DPO personnel change	October 2021
Change to details of legislation and incorporation of CCTV	April 22

Appendix 1a

Diocese of Hereford Multi-Academy Trust

Withdrawal of Consent Form – on behalf of pupil

Please complete and sign this form and deliver to the Academy office.

Please note that as a Trust we may have contractual, statutory, and/or regulatory reasons why we will still process and hold details of a pupil, parent, staff member, volunteer, or other person.

Where there is shared parental responsibility or where the pupil is capable of expressing a view and there is conflict between the individuals; the process of withdrawing consent will be subject to an evaluation and discussion. This is to enable a decision to be reached that is considered to be in the pupil's best interests

We may need to seek identification evidence and have sight of any Court Order or Parental Responsibility Agreement in some cases to action this request. If this is the case, a senior member of the Academy's staff will discuss it with you.

I withdraw consent for DHMAT to process the personal data described below in relating to the name pupil.

Name of person withdrawing consent	
Name of pupil that this withdrawal concerns	
A description of the personal data that this withdrawal concerns and for which consent was previously granted	
I confirm that I am the parent or carer of the named pupil and that I have parental responsibility for pupil	*Signed:* *Date:*

For DHMAT use only:	
Date received by DHMAT	
Name of staff member receiving withdrawal of consent form	
Record of actions taken	

Appendix 1b

Diocese of Hereford Multi-Academy Trust

Diocese of Hereford Multi-Academy Trust

Withdrawal of Consent Form – Adult

Please complete and sign this form and deliver to the Academy office.

Please note that as a Trust we may have contractual, statutory, and/or regulatory reasons why we will still process and hold details of a pupil, parent, staff member, volunteer, or other person.

I withdraw consent for DHMAT to process the personal data described below in relating to the name pupil.

Name of person withdrawing consent	
A description of the personal data that this withdrawal concerns and for which consent was previously granted	
Signed: *Date:*	

For DHMAT use only:	
Date received by DHMAT	
Name of staff member receiving withdrawal of consent form	
Record of actions taken	

Appendix 2

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

There are two distinct rights of access to information held by academies about individuals:

1. 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.
2. The right of those entitled to have access to curricular and educational records as defined within the Education Pupil Information (England)) Regulations 2005.

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 response time for Subject Access Requests for all or part of the pupil's educational record, once officially received, is 15 school days. If the subject access request does not relate to the educational record, we will respond within one month. However, the one month will not commence until after clarification of the information sought.
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 DHMAT's 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.

Further advice and information can be obtained from the Information Commissioner's Office, www.ico.gov.uk or telephone 0303 123 1113.

Diocese of Hereford Multi-Academy Trust

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. You are entitled to receive this information under the Data Protection Act 2018 (DPA) and the EU General Data Protection Regulations (GDPR), which came into effect on the 25th May 2018. We will also provide you with information about any processing of your personal data that has been carried out, the retention, which applies to your personal data, and any rights to rectification, erasure, or restriction of process that may exist.

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 3

Diocese of Hereford Multi-Academy Trust

Data Breach Procedure

This procedure is designed to ensure that all staff, LAB 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 Head teacher 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. 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.	