HERITAGE MULTI ACADEMY TRUST

EXCELLENCE THROUGH COLLABORATION

Data Protection Policy

Approved by:	Trust Board	**Date:**	07.5.26
Last reviewed on:	April 2026		
Next review due by:	April 2028		

1. Aims

Heritage MATaims to ensure that all personal data collected about staff, pupils, parents, trustees, visitors and other individuals is collected, stored and processed in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018) and the Data (Use and Access) Act 2025

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

2. Legislation and guidance

This policy meets the requirements of the UK GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO).

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.

It also reflects the updated ICO guidance on the use of surveillance cameras.

Consideration is also given to the Protection of Freedoms Act 2012 in realtion to the trust's use of biometric data.

The School's Retention and Deletion Policy is based on the IRMS Toolkit for Schools.

3. The data controller

Heritage MATprocesses personal data relating to pupils, parents, staff, trustees, visitors and others, and therefore is a data controller.

The trust has paid its data protection fee to the Information Commissioner's Office (ICO), as legally required. Our ICO registration number is Z3061884.

4. Roles and responsibilities

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

4.1. Board of Trustees

The Board of Trustees has overall responsibility for ensuring that our trust complies with all relevant data protection obligations.

4.2. Data protection officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection legislation, and developing related policies and guidelines where applicable.

The DPO is the official point of contact for individuals whose data the trust processes, and for the ICO.

Our DPO is Data Tools for Schools Limited and is contactable via the trust office.

4.3. CEO

The CEO acts as the representative of the data controller on a day-to-day basis.

4.4. Trust Data Protection Lead

The Data Protection Lead within trust is the CFO. The data protection lead acts as the point contact for the school data protection leads on all data protection issues, liaising with the DPO where necessary.

4.5. School Data Protection Leads

Each school has a data protection lead who acts as the point contact for staff and data subjects at each school. In most cases this is the School Business Manager.

4.6. All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the trust of any changes to their personal data, such as a change of address
- Contacting the DPO or Data Protection Leads in the following circumstances:
    - With any questions about the operation of this policy, data protection legislation, 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 European Economic Area (EEA)
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

5. Data protection principles

The UK GDPR is based on data protection principles that our trust must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes and not processed further in a manner that is incompatible with these purposes.
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

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

6. Data protection by design and default

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

- Appointing a DPO and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge. The DPO should have expert knowledge of data protection laws and an understanding of how to apply these in an educational context. The DPO should not be a key decision maker on how data is managed within the trust or its schools.
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 5)
- Completing data protection impact assessments where the trust's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matter; we will maintain a record of attendance for this training
- Ensuring that new members of staff have appropriate data protection training as part of their induction
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our trust and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)

- For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, any international transfers, how and why we are storing the data, retention periods and how we are keeping the data secure

7. Collecting personal data

7.1. Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the trust can **fulfil a contract** with the individual, or the individual has asked the trust to take specific steps before entering into a contract
- The data needs to be processed so that the trust can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the trust, as a public authority, can perform a task **in the public interest** or exercise its official authority
- The data needs to be processed for the **legitimate interests** of the trust (where the processing is not for any tasks the trust performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden.
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For **special categories of personal data**, we will meet one of the special category conditions for processing which are set out in the DPA 2018.

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For **criminal offence data,** we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect or use personal data in ways which have unjustified adverse effects on them.

7.2. Limitation, minimisation and accuracy

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

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

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

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

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the trust's records management policy.

8. Sharing personal data

We will share personal data if:

- There is an issue with a pupil or parent/carer that puts the safety of others at risk
- We need to liaise with other agencies – we will seek consent if 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 which can provide sufficient guarantees that they comply with 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 agencies 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 data protection law.

A record of all data sharing will be maintained.

9. Individuals rights

Individuals also have the right to:

- Access their personal data and supplementary information
- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest or legitimate interests
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach in certain circumstances
- Make a complaint to the trust and then if not happy with the trust's response to complain 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 via the school or trust office. If staff receive such a request, they must immediately inform the Data Protection Lead and DPO.

All requests to exercise an individual's rights will be acknowledged as soon as practicable and fully responded to within one month of receipt of the request. In complex cases the trust may apply an extension of up to two months.

When we refuse a request, we will tell the individual why and tell them they have the right to complain to the trust and then if not happy with the response to complain to the ICO or they can seek to enforce their rights through the courts.

9.1. Subject access requests

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

- Confirmation that their personal data is being processed
- 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
- 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

Subject access requests can be submitted by any method of communication to anybody within the organisation. The trust would prefer to receive written requests and may ask individuals to complete the request form available in Appendix 4. Requests should include the following information

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request, they must immediately forward it to the DPO, via the school or trust's Data Protection Lead.

9.1.1. 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.

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 primary schools may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.1.2. Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual to confirm the request was made and to clarify the extent of the information requested
- Will respond without delay and within 1 month of receipt of the request (or receipt of confirmation of any additional information requested and proof of identity)
- 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

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of harm, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we cannot 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 which takes into account administrative costs. We will consider whether the request is repetitive in nature when making this decision.

9.2. Rectification of personal data

Individuals are entitled to have any inaccurate or incomplete personal data rectified.

Where the personal data in question has been disclosed to third parties, the trust will inform them of the need for rectification where possible. Where appropriate, the trust will inform the individual about the third parties that the data has been disclosed to.

9.3. Erasure of personal data

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased to comply with a legal obligation

The trust has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or the exercising of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Where personal data has been made public within an online environment, the trust will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

9.4. Restriction to the processing of personal data

Individuals have the right to block or suppress the trust's processing of personal data. In the event that processing is restricted, the trust will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

The trust will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the trust has verified the accuracy of the data
- Where an individual has objected to the processing and the trust is considering whether their legitimate grounds override those of the individual

- Where processing is unlawful, and the individual opposes erasure and requests restriction instead
- Where the trust no longer needs the personal data, but the individual requires the data to establish, exercise or defend a legal claim

If the personal data in question has been disclosed to third parties, the trust will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

The trust will inform individuals when a restriction on processing has been lifted.

9.5. Right to data portability

Individuals have the right to obtain and reuse their personal data for their own purposes across different services. Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

Personal data will be provided in a structured, commonly used and machine-readable form. The trust will provide the information free of charge. Where feasible, data will be transmitted directly to another organisation at the request of the individual.

The trust is not required to adopt or maintain processing systems which are technically compatible with other organisations.

In the event that the personal data concerns more than one individual, the trust will consider whether providing the information would prejudice the rights of any other individual.

9.6. Right to object

The trust will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing
- Processing for purposes of scientific or historical research and statistics.

Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- The trust will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the trust can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Where personal data is processed for direct marketing purposes:

- The trust will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The trust cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the trust is not required to comply with an objection to the processing of the data.

9.7. Automated decision making and profiling

Individuals have the right not to be subject to a decision when:

- It is based on automated processing, e.g. profiling.
- It produces a legal effect or a similarly significant effect on the individual.

The trust will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

When automatically processing personal data for profiling purposes, the trust will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
- Using appropriate mathematical or statistical procedures.
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Securing personal data in a way that is proportionate to the risk, to the interests and rights of the individual and prevents discriminatory effects.

Automated decisions must not concern a child or be based on the processing of sensitive data, unless:

- The trust has the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest on the basis of legal statute

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. CCTV

School's that have installed a CCTV system will adhere to the ICO guidance on the use of surveillance cameras and take note of the Surveillance Camera Code of Practice. Any school's system will have a full Data Protection Impact Assessment carried out as part of the procurement process which will lead to the creation of CCTV policy for the school.

12. Biometric Recognition Systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use fingerprints to receive school dinners instead of paying with cash) we will comply with the requirements of the Protection of Freedoms Act 2012. Any use of biometric data should have the processing reviewed by the completion of a Data Protection Impact Assessment.

Parents/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 obtain the written consent of at least 1 parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric systems. We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can access the relevant service by using their pin number instead of the biometric system, if they wish.

Parents/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 parents/carers.

Where staff members or other adults use the school's biometric systems, we will also obtain their 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.

13. Photographs and videos

As part of our activities, we may take photographs and record images of individuals within our trust. Photographs and videos are an important part of recording and evidencing a child's education and will routinely be used within school and on educational activities out of school.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and 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/carers at school/trust events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Uses may include:

- Within schools on notice boards and in school/trust magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school/trust websites 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. Artificial Intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. We recognise 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, we will treat this as a data breach and will follow the personal data breach procedure outlined in Appendix 2.

15. Data security

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
- Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices and paper under lock and key and encrypting electronic data The person taking the information from the school premises accepts full responsibility for the security of the data
- National Cyber Security Centre guidance on passwords/passkeys will be followed. Staff and pupils are reminded that they should not reuse passwords from other sites. Multi-factor authentication will be enabled on all systems that hold or communicate sensitive data.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Computers and other electronic devices will be screen locked when they are not in use, this should be automated to a minimum possible time
- Staff, pupils or trustees who store personal information on their personal devices are expected to follow the same security procedures as for trust-owned equipment. (See our policies on IT security and acceptable use)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)
- Emails containing sensitive or confidential information sent by the trust are password-protected or encrypted if there are unsecure servers between the sender and the recipient

- Circular emails are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients
- Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the schools/trust containing sensitive information are always supervised
- The physical security of the trust's buildings and storage systems, and access to them, is reviewed regularly. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place
- The trust has appropriate backups of electronic data with critical data backed up offsite. Continuity and recovery measures are in place including secure copies of administrative logins and passwords to all systems

16. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will cross-shred or incinerate paper-based records and overwrite or delete electronic files. We may use a third party to safely dispose of records on the trust's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17. Personal data breaches

The trust will make all reasonable endeavours to reduce the possibility of personal data breaches. Breaches are likely to happen, and it is important that staff have an open culture and report all possible breaches and near misses.

In the event of a suspected data breach, we will follow the procedure set out in appendix 2

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school/trust context may include, but are not limited to:

- A non-anonymised dataset being published on a school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

A log detailing all breaches and associated actions and measures to prevent a recurrence will be maintained.

18. Training

All staff and trustees are provided with regular data protection training. All new staff will have role specific data protection training included in their induction process.

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

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed **every 2 years** and shared with the full trust body.

20. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Privacy notices
- Records management policy
- Safeguarding policy
- Computer acceptable use policy
- Online safety policy
- CCTV policy

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 Breach Procedure.

The trust holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This procedure applies to all personal and sensitive data held by the trust and all trust staff, trustees, volunteers and contractors, referred to herein after as 'staff'.

This breach procedure sets out the course of action to be followed by all staff at the trust if a data protection breach takes place.

Types of Breach

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Data protection breaches could be caused by a number of factors. A number of examples are shown below:

- Loss or theft of pupil, staff or governing body data and/ or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment Failure;
- Poor data destruction procedures;
- Human Error;
- Cyber-attack;
- Hacking.

Managing a Data Breach

In the event that the Trust identifies or is notified of a personal data breach, the following steps should be followed:

1. The person who discovers/receives a report of a breach must inform the Data Protection Lead in school who will inform the Trust's Data Protection Officer (DPO). If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.

2. The Data Protection Lead/DPO must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the IT technician.

3. As a registered Data Controller, it is the trust's responsibility to take the appropriate action and conduct any investigation. If the breach is felt to be significant, the Chair of Trustees should be informed.

4. The Data Protection Lead/DPO must also consider whether the police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. In such instances, advice from the Trust's legal support should be obtained.

5. The Data Protection Lead/DPO must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

- Attempting to recover lost equipment.

- Contacting the relevant Local Authority Departments, so that they are prepared for any potentially inappropriate enquiries ('phishing') for further information on the individual or individuals concerned. Consideration should be given to a global email to all trust staff. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details if possible and confirm that they

will ring the individual, making the enquiry, back. Whatever the outcome of the call, it should be reported immediately to the Data Protection Lead/DPO

- Contacting the Local Authority Communications Division if part of the crisis service, so that they can be prepared to handle any press enquiries.

- The use of back-ups to restore lost/damaged/stolen data.

- If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.

- If the data breach includes any entry codes or IT system passwords, then these must be changed immediately, and the relevant agencies and members of staff informed.

Investigation

In most cases, the next stage would be for the DPO to fully investigate the breach. The DPO should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

- The type of data;
- Its sensitivity;
- What protections were in place (e.g. encryption);
- What has happened to the data;
- Whether the data could be put to any illegal or inappropriate use;
- How many people are affected;
- What type of people have been affected (pupils, staff members, suppliers etc) and whether there are wider consequences to the breach.

A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the Information Commissioner's Office (ICO). A more detailed review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

Notification

Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an initial investigation has taken place. The DPO should decide whether anyone is notified of the breach. In the case of significant breaches, the ICO must be notified within 72 hours of the breach. Every incident should be considered on a case by case basis.

The report to the ICO should include the following information

- A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

When notifying individuals, give specific and clear advice on what they can do to protect themselves and what the Trust is able to do to help them. You should also give them the opportunity to make a formal complaint if they wish (see the Trust's Complaints Policy). The notification should include

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

Review and Evaluation

Once the initial breach management process is over, the Data Protection Lead and DPO should fully review both the causes of the breach and the effectiveness of the response to it. Reportable breaches should be reported to the next available Senior Management/Leadership Team and Board of Trustees meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put this right. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with the trust's HR provider for advice and guidance. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

Implementation

The Head Teacher/Principal/DPO should ensure that staff are aware of the Trust's Data Protection policy and its requirements including this breach procedure. This should be undertaken as part of induction, supervision and ongoing training. If staff have any queries in relation to the Trust's Data Protection policy and associated procedures, they should discuss this with their line manager, DPO or the Head Teacher/Principal.

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.
Set out the relevant actions you will take for different types of risky or sensitive personal data processed by your school. For example:

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the Data Protection Lead/DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the Data Protection Lead will ask the external IT support provider to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the Data Protection Lead/DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The Data Protection Lead will endeavour to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
- The Data Protection Lead will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted
- If safeguarding information is compromised, the Data Protection Lead will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its local safeguarding partners

Other types of breach that you might want to consider could include:

- Details of pupil premium interventions for named children being published on a school website
- Non-anonymised pupil exam results or staff pay information being shared with trustees
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked and parents' financial details stolen
- Hardcopy reports sent to the wrong pupils or families

Appendix 3 – Data Breach Report Form

Hritage MAT
Record of Data Protection Breach

Please complete the dark sections in the below form giving as much detail as possible. The form should be typed and saved and sent to the data protection lead as soon as possible

Completed by (Name):	
Job title:	
School/Organisation:	
Contact e-mail address and phone number:	
Date breach occurred:	
Date breach discovered:	
Date breach reported:	
Date investigation started:	
Date investigation completed:	
Description and nature of the breach:	
Number of Data Subjects involved:	
Volume of personal data:	
Category of personal data: *List the broad types of information*	
Further details of the personal data:	
Containment Action: *Summarise actions taken to recover from the mistake, measures taken to mitigate any possible adverse effects on the individual(s) concerned and actions taken to stop it getting worse, e.g. 'collected information', or 'asked recipient to delete it'.*	
Risks as a result of the breach: *Describe the risks or consequences; for example, if the in- formation contained financial data such as bank account numbers, then there may be a risk of fraud, or if the information contained sensitive health and personal data then there may be a safeguarding issue that could leave the affected individual vulnerable.*	

Overall impact of the breach: *Consider: Sensitivity of the data; volume of data; and; potential detriment to individuals.*	
Impact of the breach on Data Subject:	
Assess who should be notified: *List and state why - informing people and organisations that have experienced an incident can be an important element in helping to manage the situation. Notifying a person whose information got misdirected, for example, would help them to take precautions against ID theft, fraud etc. Also consider if notification would serve only to worry them without any benefit; informing people about an incident is not an end in itself. Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.*	
Notification recommendation: *Tick all those that apply, adding additional information if required. Keep a record of the notification.*	
Evaluation: *Summarise the lessons learnt.* *Measures to be taken by the school/trust to reduce the likelihood of such incidents from happening again:* *Consider adding to an action plan, with time for a review to check if measures have been implemented.*	
Senior staff sign off and recommendations:	The Head Teacher/Princpal/Chair of Trustees/DPO have read and reviewed the form and discussed the matters with relevant members of staff to reach the below conclusions: Agree/Do not agree [delete as applicable] with the assessment of risk and recommendations' The breach is not/is [delete as applicable] deemed reportable to the Information Commissioner. [Add additional points as required]
Signature:	
Name:	
Job title:	
School/Organisation	

Appendix 4 – Data Subject Rights Request Form

If you wish to make a request for personal data or to exercise any of your other rights under Data Protection legislation, please complete the form below to enable us to meet your request. The form is not mandatory; however, it will help us to respond to your request as quickly as possible. The school will endeavour to respond to your request within one calendar month. We may extend this time if the request is complex, however we will inform you of this within one month of receipt of the request, together with the reason(s) for delay.

Personal information collected from you on this form, is required to enable your request to be appropriately processed, this personal information will only be used in connection with the processing of this request.

Please note: Before logging your request, we may require proof of identity by production of a passport, photo-driving licence, or a utility bill in your name and current address.

Name		
Address		
Date of Birth:		
Contact Phone number:		
Email Address:		
Type of request (please tick)	Subject Access Request Correction of Data Erasure Request Restrict use of Data	☐ ☐ ☐ ☐
Details of request (please provide as much information as possible):		

(Please turn over and complete the other side of this form)

Parent applying on behalf of a child

If you are a parent applying for access on behalf of your child, please complete the following and tick the relevant box.

Please note that you must be able to establish that you are legally able to act on behalf of your child. This generally means that you must have parental responsibility for him or her. It should be noted that a parent can only be granted access to their child's records if this is considered to be in the child's interests.

Name of child	Date of Birth

I (Name of parent) ..... am making a request for access to records on behalf of the child named above and:

Tick as appropriate:

The child is incapable of understanding the request and I am making the request on his/her behalf ☐

The child has consented to my making this request on his/her behalf and this consent was freely given ☐

Childs signature (where consent is given)	Date

Applicants signature

I declare that the information given be me is, to the best of my knowledge correct and that I am entitled to apply for access to the information referred to above

Signature:	Date of Request:

Once the school has received all the required information, your request should be completed within one month. In exceptional circumstances where it is not possible to comply within this period you will be informed of the delay and given a timescale for when your request is likely to be met.

Please return this form to the Data Protection Officer via the school/trust office

Please note:

- The school/trust may contact you for further clarification regarding the information required.
- Once the information has been collated, you will be notified that your file is ready for collection or to be sent securely. Please indicate below whether you would like a paper copy or secure electronic copy.

Paper copy ☐ Secure electronic copy ☐

For schools use only

Form of ID Provided	Date Request Received
Date Request Acknowledged	Target Date for Completion of SAR