Data Protection Policy

Prepared By	Deputy Chief Executive, Business
Approved By	HET Board – 13 October 2021
Policy Review Date	Autumn Term 2024

Contents

1. Purpose

The UK General Data Protection Regulation (the "UK **GDPR**"), lays down rules to protect personal privacy and uphold the rights of an individual (the "**Data Protection Rules**"). The Data Protection Rules apply to anyone who "processes" (e.g. handles or has access to) personal data of an individual.

This Policy is intended to ensure that personal information is processed properly and securely and in accordance with the Data Protection Rules. It will apply to personal information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

2. Scope

This Policy applies to all individuals and schools in Hamwic Education Trust, company number 10749662 (the "**Trust**"). For the purposes of this Policy, the term "**staff**" means all employees within the Trust and their schools including permanent, fixed-term and temporary staff, as well as governors, third party representatives, agency workers and volunteers engaged with the Trust.

3. Data protection principles

The UK GDPR provides seven data protection principles, which the Trust will follow to ensure good data handling.

1) **Lawfulness, fairness and transparency**: Personal data shall be processed fairly, lawfully and in a transparent manner;
2) **Purpose limitation:** Personal data shall be obtained only for one or more specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes (unless it is for archiving purposes in the public interest, statistical purposes or scientific or historical research purposes);
3) **Data minimisation:** Personal data shall be adequate, relevant and limited to what is necessary for its processing purposes;
4) **Accuracy:** Personal data shall be accurate and where necessary kept up to date, and every reasonable step must be taken to ensure that data which is inaccurate is erased or rectified without delay;
5) **Storage limitation:** Personal data shall not be kept in a form which allows the identification of individuals for longer than is necessary for the purpose for which it is processed (unless it is solely for archiving purposes in the public interest, statistical purposes or scientific or historical research purposes and appropriate security measures have been implemented);
6) **Integrity and confidentiality:** Personal data shall be processed in a manner that ensures its security, using appropriate technical and organisational security measures, in order to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage; and
7) **Accountability:** The organisation in control of the data is responsible for compliance with the other principles and must be able to demonstrate compliance with them.

4. Responsibilities

The Trust is responsible for the activities of all of the schools in the Trust, even though some functions are delegated to school leaders and/or local governing bodies. The Trust is the legal entity responsible for the processing of personal data by the schools within the Trust and is therefore the data controller.

The data protection rules require certain organisations to appoint a Data Protection Officer ("**DPO**") giving them prescribed responsibilities. The Data Protection Officer for the Trust is Gemma Carr, Deputy CEO (Business). The DPO will have overall responsibility for monitoring the Trust's compliance with the data protection rules. The DPO's responsibilities will include, but are not limited to, the following tasks:

- Informing and advising the Trust and its employees including keeping the Trust's Board up to date with any changes to the way the schools process data;
- Taking steps to promote individuals' awareness of why the Trust need their personal information, how the Trust will use it and with whom the Trust may share it;
- Setting out clear procedures for responding to data subject rights request including subject access requests;
- Arranging appropriate data protection training for staff, governors and volunteers so they are aware of their responsibilities;
- Ensuring that staff, governors and volunteers are aware of this Policy and are following it;
- Ensuring that new software or new services for the Trust and schools are compliant, and providing advice regarding data protection impact assessments; and
- To act as the contact point for the Information Commissioner's Office (ICO) and to cooperate with the ICO.

The Trust will ensure that the DPO is provided with resources and support to fulfil all of their responsibilities. Individuals may contact the DPO regarding any issues relating to the processing of their data by the Trust or the exercise of any of their rights in relation to it. Contact details for the DPO can be found at the end of this Policy, in the 'Contact Information' section.

The Trust's Board can delegate the day-to-day responsibility for monitoring compliance with the data protection rules and this policy to the School Leader in each school, who will appoint a Data Compliance Officer ("**DCO**"). Although the DPO will have overall responsibility for monitoring the compliance of the Trust with the Data Protection Rules and this Policy, the DCO will be responsible within their school for the following tasks:

- Ensuring that individuals are made aware of the privacy notices as and when any information is collected;
- Checking the quality and accuracy of the information held by the school;
- Applying the Trust's records retention schedule to ensure that information is not held longer than necessary by the school (the schedule can be found by visiting the Trust's intranet);
- Ensuring that when information is authorised for disposal, it is done so appropriately;

- Ensuring that appropriate security measures are in place to safeguard personal information, whether it is held in paper files or electronically;
- Only sharing personal information when it is necessary, legally appropriate to do so and in accordance with the Privacy Notices; and
- Ensuring that staff in the school are aware of this Policy and are following it.

The Trust will renew its registration with the Information Commissioner's Office (ICO) if and when necessary and pay any fees due to the ICO.

4.1 Responsibilities of staff

All staff are responsible for ensuring that:

- Any personal data that they hold is kept securely;
- Personal information is not disclosed orally, in writing, via web pages or by any other means, accidentally or otherwise, to any unauthorised third party;
- Information or data about pupils is only shared with other staff as necessary and only by secure methods (such as the secure email provider); and
- Any additional associated policies and documents are complied with (see section 10).

5. Privacy notices

When any information is collected about individuals, they must be made aware of the privacy notices. The privacy notices provide information about what, why and how information is processed.

6. Processing, disclosure and sharing of information

The Trust processes personal data for a number of different purposes including:

Lawful Ground for Processing	**Examples**
Where consent is given	- Posting photographs of a pupil on the school or the Trust website - Taking fingerprints for catering purposes
Where it is necessary for the performance of a contract to which an individual is party	- An employee's bank details in order to process their pay
Where it is necessary for compliance with a legal obligation	- Passing on pupil information to the Department for Education - Passing on pupil information to the local authority
Where it is necessary to protect the vital interests of an individual	- Passing on information about a pupil's serious health condition to the NHS or a health professional where there is a risk of

	death or serious injury to that pupil or another individual
Where it is necessary for performance of a task in the public interest	- Updating and maintaining a pupil's educational record as the pupil develops and progresses - Carrying out safeguarding activities

The Trust may also share data that they hold with members of staff, relevant parents/guardians, other schools within the Trust, local authorities, the Department for Education, Ofsted, statutory bodies and other authorities where it is necessary to do so or where we are permitted to do so, e.g. for the prevention of crime, to health professionals and examination bodies or any other body that the Trust or the school deems appropriate. Any sharing of data must be in accordance with the data protection rules, this policy and the privacy notices.

If the Trust, or any of its' schools, receives enquiries from third parties, particularly by telephone, it is important to be careful about what data is disclosed. The following steps should be followed:

- Ensure the identity of the person making the enquiry is verified and check whether they are entitled to receive the information they have requested;
- Require the third party to put their request in writing in order to verify their identity and their entitlement to the data requested;
- If in doubt, refer the request to the DPO of the Trust;
- When providing information to a third party, do so only in accordance with the Data Protection Rules, the Privacy notices and this Policy; and
- Consider if a parent or guardian should have access to a pupil's information or whether the pupil is old enough to make any request themselves.

6.1 Images and biometric data

- ***Management Information System –*** Where personal information and images are stored.
- ***Websites –*** Where personal information, including images, is placed on the Trust's or the school's website, consent will be sought from the individual as appropriate.
- ***Photographs*** – Permission will be sought from the individual by the Trust or the school before photographs of the individual are used or displayed, including in the school prospectus, newsletter or any other such publication where they can be clearly identified individually.
- ***CCTV –*** Where a school uses CCTV, it is responsible for ensuring procedures for use are in compliance with the CCTV Policy, the Data Protection Policy and with the ICO guidance - https://ico.org.uk/media/1542/cctv-code-of-practice.pdf and https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/encryption/encryption-scenarios/#12

- ***Fingerprints –*** Where fingerprint records are taken from secondary pupils for catering or similar purposes, explicit consent will be sought from the individual as appropriate.
- ***Social Media –*** Where personal information, including images, is placed on the Trust or school's social media platforms e.g. Facebook/Twitter/LinkedIn, etc., consent will be sought from the individual as appropriate.

7. Request for access to information

Any person whose personal information is held by the Trust or any of its' schools has a right to ask for access to this information. These requests will be free of charge. Any requests must be made to the school's DCO or the Trust's DPO. A response to any such request will be processed within one month from the date on which the request was received.

The right to make a subject access request is the pupil's right. Parents/guardians are only entitled to access information about their child (by making a request) if the child is unable to act on their own behalf, e.g. because the child is not mature enough to understand their rights or if the child has given their consent. If you are unsure about whether or not to provide information about a pupil to a parent or guardian, please speak to your DCO or the Trust's DPO before providing any information.

Requests that fall under the Freedom of Information Act 2000 will be dealt with in accordance with the Trust's Freedom of Information Policy.

More information and detailed guidance can be found by visiting www.ico.gov.uk.

Individuals also have other legal rights under the data protection rules, including to object to and restrict processing in certain circumstances, right to have personal data erased and to have inaccurate personal data corrected. More information on these rights can be found in the privacy notices under "Requesting access to personal data".

8. Complaints and breach notification

Complaints should be made following the Trust's Complaints Procedure found on the website www.hamwic.org.

Information about how the Trust and its schools will deal with data breaches, including who staff should contact if they believe there may have been a data breach, can be found in the Trust's Data Breach Procedure (Appendix 3). The Data Protection Rules contain requirements about handling of breaches, which the Trust must comply with, so please ensure that you immediately report any potential breaches in accordance with the Data Breach Procedure.

9. Contact information

The first point of contact is the DCO for your . If the DCO is unavailable, you should contact the Trust's DPO.

The data protection registration number for Hamwic Education Trust is ZA265013. A copy of the registration can be found at https://ico.org.uk/ESDWebPages/Entry/ZA265013.

The Trust's DPO is Gemma Carr, Deputy CEO (Business), who can be contacted by email at compliance@hamwic.org, by telephone on 023 8078 6833, or at the following address:

Hamwic Education Trust, Unit E, The Mill Yard, Nursling Street, Southampton, Hampshire SO16 0AJ

10. Associated policies

- Freedom of Information Policy
- Complaints Procedure
- Acceptable Use of IT Policy

INSERT SCHOOL LOGO

Appendix 1: Pupil Photograph & Video Consent Form

PUPIL DIGITAL PHOTOGRAPHS AND/OR VIDEOS CONSENT FORM

Occasionally, we may take photographs of the pupils at our school. We may use these images in our school's prospectus, other printed publications, websites, social media platforms (e.g. Facebook, Twitter, etc.) and/or on display boards.

We may also take videos for educational use and/or use as evidence for Ofsted. These videos may potentially also be used in websites, social media platforms and display screens.

Hamwic Education Trust may also use the photographs/videos of pupils in publications, publicity materials and internet platforms.

We may also send the images to the news media (or they may come into the school and take pictures/videos), who may use them in printed publications and on their website, and store them in their archive. They may also syndicate the photos to other media for possible use, either in printed publications, or on websites, or both. When we submit photographs and information to the media, we have no control on when, where, if or how they will be used.

Terms of Use

- We will take all reasonable measures to ensure the images are used solely for the purposes for which they are intended. However, we cannot guarantee this and take no responsibility for the way images are used by other websites or publishers, or for any consequences arising from publication.
- We will not use the personal details of a pupil, including their full name, alongside a photographic image on our website, in our school prospectus or in any other printed publications without good reason, for example, we may include the full name of a pupil in a newsletter to parents if the pupil has won an award.
- If we name a pupil in the text, we will not use a photograph of that child to accompany the article without good reason.
- We will make every effort to ensure that we do not allow images to be taken of any children for whom we do not have permission or who are 'at risk' or disallowed from having their photographs taken for legal or social reasons.
- We may use group or class photographs or footage with very general labels e.g. 'maths lesson'.

Consent

I give permission for my child's image to be used in school e.g. Bromcom/SIMS, Books, Notice Boards, etc.	YES / NO

I give permission for my child's image to appear in the school prospectus and/or other printed publications that the school or Trust produce for promotional purposes.	YES / NO
I give permission to the school and Trust to use my child's image on school/Trust websites.	YES / NO
I give permission to the school to use images of my child in notifications via social media (to include Twitter/Facebook) to share details of school events and activities.	YES / NO
I give permission for you to record my child's image on video or webcam to be displayed online via school or other websites.	YES / NO
I give permission for images of my child to be used by the news media in printed and/or electronic form and stored in their archives. This might include images sent to the news media by the school and images/footage the media may take themselves if invited to the school to cover an event.	YES / NO

I have read and understood the above information.

Pupil Name:	Year Group
Parent Name:	Parent Signature:
Date:	

Appendix 2: Staff Photograph & Video Consent Form

STAFF DIGITAL PHOTOGRAPHS AND/OR VIDEOS CONSENT FORM

Occasionally, we may take photographs of staff at our school or Trust. We may use these images in our school's prospectuses, other printed publications, websites, social media platforms (e.g. Facebook, Twitter, etc.) and/or on display boards.

We may also take videos for educational use and/or use as evidence for Ofsted. These videos may potentially also be used in websites, social media platforms and display screens.

Hamwic Education Trust may also use the photographs/videos of staff in publications, publicity materials and internet platforms.

We may also send the images to the news media (or they may come into the school and take pictures/videos), who may use them in printed publications and on their website, and store them in their archive. They may also syndicate the photos to other media for possible use, either in printed publications, or on websites, or both. When we submit photographs and information to the media, we have no control on when, where, if or how they will be used.

Terms of Use

- We will take all reasonable measures to ensure the images are used solely for the purposes for which they are intended. However, we cannot guarantee this and take no responsibility for the way images are used by other websites or publishers, or for any consequences arising from publication.
- We will make every effort to ensure that we do not allow images to be taken of any staff for whom we do not have permission or who are 'at risk' or disallowed from having their photographs taken for legal or social reasons.
- We may use group or class photographs or footage with very general labels e.g. 'maths lesson'.

Consent

I give permission for my image to be used in school e.g. SIMS/Bromcom, Books, Notice Boards, etc.	YES / NO
I give permission to the school and Trust to use my image on school/Trust websites.	YES / NO
I give permission to the school to use images of me in notifications via social media (to include Twitter/Facebook) to share details of school events and activities.	YES / NO
I give permission for you to record my image on video or webcam to be displayed online via school or other websites.	YES / NO
I give permission for images of me to be used by the news media in printed and/or electronic form and stored in their archives. This might include images sent to the news media by the school and images/footage the media may take themselves if invited to the school to cover an event.	YES / NO

I have read and understood the above information.

Staff Name:	Staff Signature:
Date:	

Appendix 3: Data Breach Procedure for Hamwic Education Trust (the "Trust") and its schools

1. About this procedure

This procedure describes the actions that must be taken by staff to report any incident which may result in a personal data breach. A "personal data breach" is defined in Article 4(12) of the UK General Data Protection Regulation as:

"A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

Often, when an incident first comes to light, it will not be possible to determine whether or not it constitutes a personal data breach. The term "incident" is used in this policy to describe any situation which may, upon investigation, turn out to be a personal data breach.

This policy should be read in conjunction with the Data Protection Policy which can be found on the Trust's website (www.hamwic.org) or on the Trust's intranet.

2. Identifying an incident

An incident may come to light in a number of ways. For example, it could occur by:

- direct observation e.g. where a member of staff spots that personal data has been sent to the wrong email address;
- being reported to us by a pupil or parent: e.g. where a pupil notifies us that she/he has received personal data relating to another pupil;
- being reported to us by another party, such as a contractor, a local authority or a member of the public;
- compromise of your personal account through either phishing, ransomware or other form of cyber attack;
- an audit / review revealing that an incident had occurred

3. Actions to take once an incident has been identified

Whenever an incident is identified, the following actions must be taken:

	Action	**Responsibility**	**Timelines**
1.	Report the incident to the data compliance officer for the school (or, if unavailable, the Data protection officer of the Trust)	Member of staff who was first made aware of the incident	**Immediately after the incident is identified**
2.	Investigate and identify the full details of the incident to identify the cause	Data compliance officer for the school (with the assistance of the colleague	**As soon as possible following the incident**

		who reported the incident)	**being reported**
3.	Identify any remedial action (see section 4, below)	Data compliance officer for the school	**As soon as possible following the incident being reported**
4.	Complete a formal Personal Data Breach Form online at incidents.hamwic.org, which will notify the DPO	Data compliance officer for the school	**Within 48 hours of the incident being identified**
5.	Review the Personal Data Breach Form and determine whether the incident constitutes a personal data breach or a 'near miss' (i.e. an incident which does not meet the definition of a personal data breach)	Data protection officer (in conjunction with the data compliance officer for the school)	**As soon as possible following step 4**
6.	If necessary, decide whether to notify (i) the ICO; and/or (ii) individual data subjects, of the personal data breach (see section 5, below)	Data protection officer (in conjunction with the data compliance officer for the school)	**As soon as possible following step 4**
7.	If necessary, notify the ICO of the personal data breach	Data protection officer	**Within 72 hours of the incident being identified**
8.	If necessary, notify individual data subjects of the personal data breach	Data compliance officer / data protection officer	**Without undue delay (in practice this should be done as soon as possible)**

Please note all incidents should be reported to the Trust via the online GDPR Breach Form found at incidents.hamwic.org on the Trust Intranet. If any advice is needed, the DCO should email compliance@hamwic.org.

4. Taking remedial action

Following the reporting of the issue, the Trust's data protection officer shall advise the relevant data compliance officer what remedial action must be taken, in particular where pupils or parents are affected in any way by the personal data breach. Pupils or parents may suffer distress and inconvenience where they are aware that a breach has occurred. In some cases, they may be at risk of suffering financial detriment or physical harm as a result of the breach.

Remedial action should seek to mitigate any risks the pupil or parent has been exposed to as a result of the breach, to prevent similar breaches occurring in the future and to protect the Trust's and the school's reputation. Action will be dependent on case specifics, but the data protection officer should consider the Trust's responsibility to act in the best interests of pupils and parents.

If there is any doubt at all about the remedial action required to be taken, the data compliance officer must contact the Trust's data protection officer.

Remedial action might include the following:

- if personal data is in the hands of a third party, it should be retrieved from the third party or deleted from the third party's IT system (please speak to the managed services IT team for assistance);
- if the breach arose as a result of an IT issue, the source of the issue should be identified and rectified (please speak to IT for assistance);
- if the breach arose as a result of human error, the individual should be made aware of the error and where appropriate asked to undertake additional training

5. Notifying a personal data breach

Under the UK General Data Protection Regulation, there is an obligation to report a personal data breach to the Information Commissioner's Office (ICO) 'without undue delay' and in any event within 72 hours of us becoming aware of the breach.

There is an exception to this reporting requirement where the personal data breach is unlikely to result in a risk to the rights and freedoms of the individuals affected. A decision on whether the breach must be reported to the ICO will be made by the Trust's data protection officer following receipt of the personal data breach form.

Where the personal data breach is likely to result in a high risk to the rights and freedoms of individuals affected, there is an obligation to notify those individuals of the breach 'without undue delay'. A personal data breach that may result in a high risk to individuals may include where a parent is exposed to the risk of suffering financial detriment or physical harm if they are not notified of the breach. Where this is the case, then the school data compliance officer or Trust's data protection officer must inform them of the breach by letter and issue a formal apology. The Trust's data protection officer will make the final decision as to whether notifying individuals is required.

Where pupils or parents are aware that they are the subject of a personal data breach, then they must be issued with a written apology. Brief details of the remedial action taken should be provided to reassure them, where this information can be provided without revealing any personal or confidential information.

Where appropriate, remedial action should also consider anyone other than the pupil(s) or parent(s) who may also have been affected indirectly. These individuals should also be sent a written apology to minimise the Trust's reputational damage.

As well as the requirement to report personal data breaches to the ICO, it may also be necessary to report them to other authorities such as the police. These actions should only be undertaken following consultation with the Trust's data protection officer.

6. Follow-up action

To ensure that we learn from our mistakes, the school responsible is required not only to confirm that

remedial action has taken place, but also that the causes of the personal data breach have been analysed and action taken to ensure similar breaches do not occur again. Confirmation of this action is reported and saved by the Trust's data protection officer as an audit trail.

7. Central logging of the issue

Once the school responsible has confirmed remedial action and any appropriate follow-up action, then, subject to:

- the pupil(s) or parent(s) being satisfied with the remedial action taken in respect of the breach and;
- the data protection officer being satisfied that regulatory procedures have been followed,

the breach can be marked as closed by the data protection officer.

A copy of all breach forms will be kept by the data protection officer and stored at the Trust's head office.