

# Data Protection Policy

Gemma Carr, Deputy CEO, Business & DPO

HET Board

September 2021

Ongoing

September 2024

---

.....	3
.....	3
.....	3
.....	3
.....	4
.....	5
.....	5
.....	6
.....	6
.....	6
.....	7
.....	7
Appendix 1: Pupil Photograph & Video Consent Form .....	8
Appendix 2: Staff Photograph & Video Consent Form .....	10
Appendix 3: Data Breach Procedure for Hamwic Education Trust (the "Trust") and its schools .....	11



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 r





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.

Where personal information and images are stored.

Where personal information, including images, is placed on the Trust's or the school's website,



The first point of contact is the DCO for your school (INSERT DCO NAME AND EMAIL). If the DCO is unavailable, you should contact the Trust's DPO.



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.

---

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





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



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.

---

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'.

---

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	



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](http://www.hamwic.org)) or on the Trust's intranet.

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

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

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	
2.	Investigate and identify the full details of the incident to identify the cause	Data compliance officer (DCO) for the school (with the assistance of the colleague who reported the incident)	
3.	Identify any remedial action (see section 4, below)	DCO for the school	
4.	Complete a formal Personal Data Breach Form online at <a href="http://incidents.hamwic.org">incidents.hamwic.org</a> , which will notify the DPO	DCO for the school	
5.	Review the Personal Data Breach Form and determine whether the incident constitutes a	Data protection officer (DPO) (in conjunction with the DCO for the	



	personal data breach or a 'near miss' (i.e. an incident which does not meet the definition of a personal data breach)	school)	
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)	DPO (in conjunction with the data compliance officer for the school)	
7.	If necessary, notify the ICO of the personal data breach	DPO	
8.	If necessary, notify individual data subjects of the personal data breach	DCO / DPO	

---

Following the reporting of the issue, the Trust's DPO 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 si



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 DPO 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.

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.

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 DPO.

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

