Data Protection Policy

Reviewed on	September 2026	Review frequency	Annual
Next review due	September 2027	Template Yes / No	Yes
Owner	Head of Safeguarding and Compliance	Approved by	DCEO

1. History of Policy Changes

Date	Page	Change	Origin of Change
Sept 26	4-5	Updated definitions and legislative references, including Data (Use and Access) Act 2025.	Legislative update
	6	Data Protection Commitments reformatted and strengthened.	Policy review
	6-7	Data Protection Principles expanded, including stronger wording on transparency, purpose limitation, minimisation and security.	Legislative clarification and policy review
	7-9	Legal Grounds for Processing updated. Explicit reference added to Vital Interests and revised lawful basis wording.	Legislative update
	9	Added right to data portability	Legislative update
	10	Strengthened Data Security controls and disposal requirements.	Policy review
	11	New Automated Decision-Making and Profiling section.	New technology and legislative development
	13	Personal Data Breaches section updated.	Policy review
	13	Disclosure and Sharing section updated.	Policy review

2. Contents

1. History of Policy Changes 2
2. Contents 3
3. Aims 4
4. Policy statement 4
5. Scope 5
6. Definitions 5
7. Data protection officer 7
8. Our data protection commitments 8
9. Data protection principles 8
10. Legal grounds for processing 9
11. Data subjects' rights 10
12. Automated decision-making and profiling 12
13. Data security 12
14. Personal data breaches 13
15. Disclosure and sharing of personal information 13
16. Data processors 14
17. Images and videos 14
18. CCTV 15
19. Biometric data 15
20. Complaints 15
21. Changes to this policy 16
22. Link to other HET policies 16
23. Annex 1: Parent and Carers Consent Form 17
24. Annex 2: Staff Consent Form 19



3. Aims

Hamwic Education Trust (HET) believe that all pupils should receive a high quality, enriching, learning experience in a safe and inclusive environment, which promotes excellence through a broad curriculum that prepares them for their future and opens doors to a diverse array of opportunities as well as that all pupils and adults within HET flourish as individuals and together.

4. Policy statement

Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities as an academy trust (Trust"), we will collect, store, and process personal data about our pupils, workforce, parents, and others. This makes us a data controller in relation to that personal data.

We are committed to the protection of all personal data and special category personal data.

The law imposes significant fines for failing to lawfully process and safeguard personal data. This policy sets out how we comply with the relevant legislation. Breaches of this policy can result in the risk of real harm to individuals, action for damages, loss of trust and reputational harm as well as regulatory penalties, including fines.

All data users must comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary or other action. Individuals may be prosecuted for committing offences under sections 170-173 of the Data Protection Act 2018.

5. Scope

The types of personal data that we may be required to handle include information about pupils, parents, our workforce, and others that we deal with. The personal data which we hold is subject to certain legal safeguards specified in the retained EU law version of the General Data Protection Regulation ((EU)2016/679) ('UK GDPR'), the Data Protection Act 2018, and other regulations (together 'data protection legislation').

This policy and any other documents referred to in it set out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

This policy does not form part of any employee's contract of employment and may be amended at any time.

This policy sets out rules on data protection and the legal conditions that must be satisfied when we process personal data.

6. Definitions

All defined terms in this policy are indicated in bold text, and a list of definitions is included below:

- **'HET',** refers to the central operations of the Hamwic Education Trust alongside any HET school within our Multi Academy Trust.
- **Biometric data,** information about a person's physical or behavioural characteristics or features that can be used to identify them and is obtained or recorded for the purposes of a biometric recognition system and can include fingerprints, hand shapes, features of the eye, or information about a person's voice or handwriting.
- **Biometric recognition system,** is a system that operates automatically (electronically) and:
  - Obtains or records information about a person's physical or behavioural characteristics or features; and
  - Compares or otherwise processes that information with stored information in order to establish or verify the identity of the person or otherwise determine whether they are recognised by the system.
- **DCO,** Data Compliance Officer in each school
- **DPO,** Data Protection Officer for HET (see section 4)
- **Data,** information, which is stored electronically on a computer, or in certain paper-based filing systems.
- **Data subjects,** for the purpose of this policy includes all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.
- **Personal data,** information relating to an identified or identifiable natural person (a data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- **Data controllers**, people who, or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with data protection legislation. We are the data controller of all personal data used in our business for our own commercial purposes.

- **Data users,** those of our workforce (including governors and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy, and any applicable data security procedures, at all times.
- **Data processors**, any person or organisation that is not a data user that processes personal data on our behalf and on our instructions.
- **Data protection legislation,** all applicable data protection and privacy legislation in force from time to time in the UK including the UK GDPR and the Data Protection Act 2018 (DPA 2018) (and regulations made thereunder) (as amended by the Data (Use and Access) Act 2025; and the Privacy and Electronic Communications Regulations 2003 (SI 2003 No. 2426) as amended, and all other legislation and regulatory requirements in force from time to time which apply to the use of personal data.
- **Data protection impact assessment (DPIA)**, a tool to help identify how to comply with data protection obligations and protect individuals' rights as set out in Article 35 of the UK GDPR. The ICO also has guidance on DPIA's on their website at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/.
- **Information Commissioner's Office (ICO),** in the UK, the Information Commissioner's Office (ICO) is the data protection regulator. The website of the ICO is at www.ico.org.uk.
- **Personal data breach,** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.
- **Privacy notices,** where we collect information either directly or indirectly from data subjects, we provide them with a statement of fair processing, referred to as a privacy notice. This notice will contain information about: our identity and contact details as data controller and those of the DPO, the purpose, or purposes, and legal basis for which we intend to process that personal data, the types of third parties, if any, with which we will share, or to which we will disclose that personal data, whether the personal data will be transferred outside the UK and if so, the safeguards in place, the period for which their personal data will be stored, by reference to our Records Management and Retention Policy, the existence of any automated decision making in the processing of the personal data along with the significance and envisaged consequences of the processing and the right to object to such decision making, and the rights of the data subject to object to or limit processing, request information, request deletion of information or lodge a complaint with the ICO.
- **Processing,** any activity that involves use of the data. It includes obtaining, recording, or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties.
- **Special category personal data,** information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, sexual orientation or genetic or biometric data.
- **Workforce,** any individual employed by HET such as staff and those who volunteer in any capacity including Trustees, Members, Governors and parent helpers.

7. Data protection officer

As a Trust, we are required to appoint a data protection officer ("**DPO**").

Our DPO is Gemma Carr (Deputy CEO) who can be contacted in the following ways:
Email: compliance@hamwic.org
Telephone: 023 8078 6833
Address: Hamwic Education Trust, Unit E, The Mill Yard, Nursling Street, Southampton, Hampshire SO16 0AJ

The DPO is responsible for informing and advising HET about data protection legislation, ensuring compliance with the data protection legislation and with this policy. Any questions about the operation of this policy, or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

The DPO is also the central point of contact for all data subjects, the Information Commissioner's Office ("ICO") and others in relation to matters of data protection.

The HET Board delegate the day-to-day responsibility for monitoring compliance with the data protection rules in 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 HET with the data protection rules of 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 HET's records retention policy to ensure that information is not held longer than necessary.
- 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.
- Ensuring that staff in the school are aware of this policy and are following it.

The first point of contact is the Data Compliance Officer for your school; their contact details are:
Name: Mrs Tamsin Sandford
Email address: hr@springdale.poole.sch.uk

If the DCO is unavailable, you should contact the HET DPO or HET Compliance Team.

All HET 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 HET policies and documents are complied with.

8. Our data protection commitments

We are dedicated to ensuring that personal data is processed in alignment with the legal principles of data protection.

We implement a strategy focused on “Data Protection by Design and Default”.

We can prove our adherence to data protection legislation.

Data subjects are well informed about how and why we use their data, and they can exercise their rights regarding their data.

We share personal data only when it is fair and lawful, ensuring that any data sharing is conducted securely.

We handle and report all personal data breaches, including minor ones, effectively to mitigate any potential risks and to improve our practices

9. Data protection principles

Anyone processing personal data must comply with the data protection principles. We will comply with these principles in relation to any processing of personal data by HET.

The principles provide that personal data must be:

- Processed fairly, lawfully, and transparently in relation to the data subject. This means that we only use personal data with respect for the individual who it relates to, in line with the legal grounds for processing, and we inform data subjects on how their personal data is processed including, among other ways, in our privacy notices.
- Processed for specified, explicit, and legitimate purposes, and in a way which is not incompatible with those purposes. This means that if we collect personal data for one purpose and then need to use it for another reason, we will ensure that new purpose is compatible with the original reason for processing.
- Adequate, relevant, and not excessive for the purpose. This means that we will collect enough information to achieve our aim, whilst minimising that collection to what is genuinely required.
- Accurate and up to date. This means that we will try to ensure that personal data is accurate when we collect it and kept up to date over time.
- Not kept for any longer than is necessary for the purpose. This means that we will only keep personal data for as long as is necessary in accordance with our [Data Retention Policy]; and
- Processed securely using appropriate technical and organisational measures. Our measures include; technical safeguards like security of ICT systems, control over ICT access, the use of pseudonyms and encryption, as well as organisational safeguards, including plans for business continuity, securing our premises and data physically, implementing policies and procedures, conducting regular training, and carrying out audits and evaluations of operational measures and strategic oversight of compliance.

Personal data must also:

- Be processed in line with data subjects' rights.
- Not be transferred to people or organisations situated in other countries without adequate protection.

10. Legal grounds for processing

For personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in the data protection legislation. We will normally process personal data under the following legal grounds:

- Where the processing is necessary for the performance of a contract between us and the data subject, such as an employment contract.
- Where the processing is necessary to comply with a legal obligation that we are subject to.
- Where the processing is necessary in order to protect the vital interests of a data subject or another individual.
- Where the law otherwise allows us to process the personal data, or we are carrying out a task in the public interest.
- Where the processing is necessary for the purposes of a recognised legitimate interest as set out in Annex 1 of the GDPR.
- Where we are pursuing legitimate interests, (or the legitimate interests of a third party), except where such interests are overridden by the interests or fundamental rights and freedoms of data subjects; and
- Where none of the above apply, then we will seek the consent of the data subject to the processing of their personal data.

When special category personal data is being processed, then an additional legal ground must apply to that processing. We understand that for certain types of processing of special category personal data, we must have, and comply with, an appropriate policy document. Our special category personal data policy is our appropriate policy document for these purposes.

We will normally only process special category personal data under following legal grounds:

- Where the processing is necessary for employment law purposes, for example, in relation to sickness absence.
- Where the processing is necessary for reasons of substantial public interest, for example, for the purposes of equality of opportunity and treatment.
- Where the processing is necessary for health or social care purposes, for example, in relation to pupils with medical conditions or disabilities; and
- Where none of the above apply, then we will seek the explicit consent of the data subject to the processing of their special category personal data.

We will inform data subjects of the above matters by way of appropriate privacy notices, which shall be provided to them when we collect the data, or as soon as possible thereafter, unless we have already provided this information such as at the time when a pupil joins us.

If any data user is in doubt as to the legal ground for processing personal data for any purpose, then they must contact the DPO before doing so.

Vital interests

There may be circumstances where it is considered necessary to process personal data or special category personal data in order to protect the vital interests of a data subject. This might include medical emergencies where the data subject is not able to give consent to the processing. We believe that this will only occur in very specific and limited circumstances. In such circumstances, we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur.

Consent

Where none of the other bases for processing set out above apply, then HET must seek the consent of the data subject before processing any personal data for any purpose.

There are strict legal requirements in relation to the form of consent that must be obtained from data subjects.

When pupils and or our Workforce join HET, a consent form will be required to be completed in relation to them (see Annex 1 and 2). This consent form deals with the taking and use of photographs and videos of them, amongst other things. Where appropriate third parties may also be required to complete a consent form.

In relation to all pupils, we will seek consent from an individual with parental responsibility for that pupil.

We will obtain written consent for photographs and videos to be taken of our pupils 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.

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.

If consent is required for any other processing of personal data of any data subject, then the form of this consent must:

- Inform the data subject of exactly what we intend to do with their personal data.
- Require them to positively confirm that they consent – we cannot ask them to opt out rather than opt in; and
- Inform the data subject of how they can withdraw their consent.

Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a data subject giving their consent. We will ensure that it will be as easy for the data subject to withdraw their consent as it was to give it.

Consent may need to be refreshed where we need to process the personal data for a different and incompatible purpose, which was not disclosed when the consent was first considered by the data subject.

The DPO must always be consulted in relation to any consent form before consent is obtained.

A record must always be kept of any consent, including how it was obtained and when.

11. Data subjects' rights

In addition to the right to be informed and the right to withdraw consent, we will process all personal data in line with data subjects' rights, in particular their right to:

- Request access to any personal data we hold about them.
- Object to the processing of their personal data, including the right to object to direct marketing.
- Have inaccurate or incomplete personal data about them rectified.
- Restrict processing of their personal data.
- Have personal data we hold about them erased.

- Have their personal data transferred; and
- Object to the making of decisions about them by automated means.

The rights available to data subjects will depend on the lawful basis for processing, for example, where personal data is processed under the lawful basis of public task, then the data subject cannot withdraw consent for such processing, but they can exercise the right of objection.

Except for the right to object to direct marketing, other rights requests in an education or employment context can be complex. We will comply with our obligations under data protection legislation and the guidance given by the ICO in respect of individuals seeking to exercise their rights.

We will consider data subject requests and provide a response within one month, except if we consider the issue to be too complex to resolve within that period, then we may extend the response period by a further two months. If this is necessary, then we will inform the data subject within one month of their request that this is the case.

Where we are unable to grant data subjects any requests made as part of their rights, for example, where we are unable to delete data as we are required to retain it in relation to any claim or legal proceedings, we will explain to the data subject why this is the case. In those circumstances we will inform the data subject of their right to complain to HET and to the ICO at the time that we inform them of our decision in relation to their request.

The DPO must be consulted in relation to any data subject rights request.

The right of access to personal data

Data subjects may request access to the personal data we hold about them and which we are able to provide based on a reasonable and proportionate search for that personal data. Such requests will be considered in line with HET's subject access request procedure.

Data protection by design and default

HET will consider and comply with the requirements of data protection legislation in relation to all of its activities whenever these involve the use of personal data, in accordance with the principles of data protection by design and default.

In certain circumstances, where the law requires us to, we shall carry out detailed assessments of proposed processing in a data protection impact assessment ("DPIA"). This includes where we intend to use new technologies which might pose a high risk to the rights of data subjects because of the types of data we will be processing, or there is a change in our existing ways of working.

HET will complete a DPIA of any such proposed processing, and has a template document, which ensures that all relevant matters are considered. We may also carry out DPIA's where one is not legally required, as a matter of good practice.

The HET Compliance Team should always be consulted as to whether a DPIA is required, and if so, how to undertake that assessment. They must always be consulted where personal data is to be transferred to different countries to ensure adequate protection is in place.

12. Automated decision-making and profiling

HET does not routinely make decisions about individuals solely by automated means. Examples of automated processing that may be used within an educational setting include:

- Admissions systems applying oversubscription criteria.
- Recruitment systems filtering or scoring applications.
- Behaviour or safeguarding systems identifying patterns or risks.
- Assessment platforms that automatically mark or analyse pupil performance.

Where automated processing produces outcomes that inform or influence decisions, HET will seek to ensure that meaningful human involvement such as review, oversight, or the ability to amend outcomes, is applied as part of the decision-making process.

Where a decision is made solely by automated means and produces legal or similarly significant effects on a data subject, the data subject has the right to:

- Be informed that such a decision has been made.
- Make representations about the decision.
- Request that a human review the decision; and
- Contest the outcome of the decision.

HET will ensure that appropriate processes are in place to receive and respond to such requests in a timely manner.

Where automated decision-making involves the processing of special category personal data, such processing will only take place where:

- The individual has given explicit consent; or
- The processing is necessary for reasons of substantial public interest and is either: (i) necessary for entering into, or performing, a contract between the individual and a controller; or (ii) required or authorised by law.

HET will keep its approach to automated decision-making under review and will seek further advice where necessary, particularly in relation to new technologies or AI-based systems. Where HET's processing activities are also subject to EU GDPR, individuals may hold broader rights in this area, and HET's privacy notices will reflect the applicable legal framework accordingly.

13. Data security

We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.

Security procedures include:

- Methods of disposal. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required. IT assets must be disposed of in accordance with the ICO guidance on the disposal of IT assets.
- Equipment. Data users must ensure that individual monitors do not show confidential information to passers-by, and that they log off from their PC when it is left unattended.

- Document printing. Documents containing personal data must be collected immediately from printers and not left on photocopiers.
- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are stored securely when not in use within locked offices or locked cabinets.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access.
- There are entry controls in all schools and any non-authorised person seen in an entry-controlled area will be challenged by a member of staff.
- Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
- Paper documents/records containing confidential or sensitive information should be securely disposed of in line with our Records Management and Retention Policy.
- Digital storage devices should be physically destroyed when they are no longer required. IT assets must be disposed of in accordance with the Information Commissioner's Office (ICO) guidance on the disposal of IT assets.
- Staff, pupils or governors who store personal information on any personal devices are expected to follow the same security procedures as for school-owned equipment. See HET specific online safety policy / ICT policy / acceptable IT use agreement / policy on acceptable use of IT.
- HET staff are encouraged to utilise the HET Cloud storage solution rather than removable media storage.
- 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.
- Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.
- Documents containing personal data must be collected immediately from printers and not left on photocopiers.

Any member of staff found to be in breach of the above security measures may be subject to disciplinary action.

14. Personal data breaches

HET recognises that a breach of personal data could happen, despite our policies, procedures, and measures in place to protect personal data, and we will respond to any breach as quickly as possible in order to minimise any risks or potential harm to individuals.

HET has a personal data breach procedure, and this must be followed in relation to any actual or suspected breach of personal data.

15. Disclosure and sharing of personal information

We may share personal data that we hold about data subjects, and without their consent, with other organisations. Such organisations include the Department for Education, Ofsted, health authorities and professionals, the local authority, examination bodies, other schools, and other organisations where we have a lawful basis for doing so.

HET will inform data subjects of any sharing of their personal data unless we are not legally required to do so, for example where personal data is shared with the police in the investigation of a criminal offence.

Where necessary, we will enter into a data sharing agreement to help facilitate the safe sharing of personal data.

In some circumstances we will not share safeguarding information. Please refer to our child protection policy.

16. Data processors

We contract with various organisations who provide services to HET. These include people, companies, and systems that process personal data on our behalf and under our instruction.

In order that these services can be provided effectively, we are required to transfer personal data of data subjects to these data processors.

Personal data will only be transferred to a data processor if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to the satisfaction of HET. HET will always undertake due diligence of any data processor before transferring the personal data of data subjects to them.

Contracts with data processors will comply with data protection legislation and contain explicit obligations on the data processor to ensure compliance with the data protection legislation, and compliance with the rights of data subjects.

17. Images and videos

Parents and others attending HET or school events are allowed to take photographs and videos of those events for personal and domestic purposes. For example, parents can take video recordings of a school performance involving their child. HET does not prohibit this as a matter of policy. However, please appreciate that this needs to be reviewed by schools considering each event and those attending. In cases where attendees are instructed that recording is not allowed, we politely request that parents and other visitors respect this instruction.

HET does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part, outside of the ability of HET to prevent.

HET asks that parents and others do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos.

Whenever a pupil begins their attendance at a HET school, they, or their parent where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that pupil. Images and videos of pupils may be required for safeguarding, assessment, and learning purposes and we will not seek consent for the taking and use of these images.

However, HET want to celebrate the achievements of our pupils and therefore may want to use images and videos of our pupils within promotional materials, or for publication in the media such as local, or even national, newspapers covering school events or achievements.

We will seek the consent of parents, and pupils where appropriate, before allowing the use of images or videos of pupils for such purposes.

18. CCTV

HET operates a CCTV system, please refer to the HET CCTV policy.

HET uses CCTV in various locations around school sites (inside and outdoors) for security, safeguarding and health and safety purposes. We adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the DCO at the school.

19. **Biometric data**

In our secondary schools, HET operates a biometric recognition system for the catering purposes.

Before we are able to obtain the biometric data of pupils or the workforce, we are required to give notification and obtain consent for this special category data due to additional requirements for processing such data under the data protection legislation and/or Protection of Freedoms Act 2012.

For the workforce, explicit written consent will be obtained at the commencement of their position within HET and shall continue to be effective unless an objection in writing to the processing of the biometric data is received from the individual.

For our pupils, the school will notify each parent of that pupil prior to them commencing their education at the school, of the use of our biometric recognition system. The school will then obtain the written consent of one of the pupil's parents before obtaining any biometric data.

In the event that written consent cannot be obtained from a parent, or any parent objects in writing, or the pupil objects or refuses to participate in the processing of their biometric data, HET will not process the pupil's biometric data and will provide the following alternative means of accessing the above services:

Further information about this can be found from schools and in our Privacy Notices.

20. Complaints

Data subjects have the right to make a complaint to the school and HET if they consider we have not complied with data protection legislation.

Any complaints relating to data protection should be directed to the school DCO in the first instance, and if unsatisfied with the response, to the HET DPO.

When dealing with complaints relating to data protection sent to HET, we shall:

- Acknowledge receipt of the complaint within 30 days of the date on which the complaint is received by HET.
- Take appropriate steps to respond to the complaint, including making enquiries into the subject matter of the complaint, to the extent appropriate.
- Inform the complainant about progress of the complaint; and
- Inform the complainant of the outcome of the complaint.

21. Changes to this policy

We may change this policy at any time. Where appropriate, we will notify data subjects of those changes.

22. Link to other HET policies

- Acceptable Use of IT Policy
- Child Protection and Safeguarding Policy
- Complaints Procedure
- Freedom of Information Policy
- Online Safety Policy
- Privacy Notices
- Records Management and Retention Policy
- Visitor Code of Conduct

23. Annex 1: Parent and Carers Consent Form

PARENT AND CARERS 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 and/or on display boards.

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

Hamwic Education Trust (HET), see definition in our Data Protection Policy, may also use these videos and images in their publications, publicity materials and social media platforms.

We may also send the images to the news media (or they may come into the school and take pictures and 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 agree for my child's images to be published on the school and HET website.	YES / NO
I agree for my child's images to be published on the school and HET social media pages.	YES / NO
I agree for my child's image to be published in a school or HET newsletters and any other printed document/publication such as a prospectus.	YES / NO
I agree for my child's images to be used in both school and HET promotional materials.	YES / NO
I agree for my child's images to be published in the media.	YES / NO
I agree for my child to have individual photographs taken by the external school photographer for purchase	YES / NO
I agree for my child to be included in group photographs taken by the external school photographer for purchase and for display within the school site	YES / NO

I have read and understood the above information.

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

24. Annex 2: Staff Consent Form

STAFF CONSENT FORM

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

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

Hamwic Education Trust (HET), see definition in our Data Protection Policy, may also use these videos and images in their publications, publicity materials and social media platforms.

We may also send the images to the news media (or they may come into the school and take pictures and 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 taken and used in school for purposes such as an ID card, Bromcom, Books, Notice/Display Boards, etc.	YES / NO
I give permission for my image to be published in a school or HET newsletters and any other printed document/publication such as a prospectus.	YES / NO
I give permission for my image to be published on the school and HET website.	YES / NO
I give permission for my image to be published on school and HET social media pages.	YES / NO
I give permission for my image to be published in the media.	YES / NO
I give permission for my image to be taken by an external school photographer	YES / NO

I have read and understood the above information.

Staff Name:	Staff Signature:
Date:	