



Protection of Biometric Information Policy

Reviewed on	Aug 2026	Review frequency	Annually
Next review due	Aug 2027	Template Yes / No	No
Owner	Director of IT	Approved by	Executive



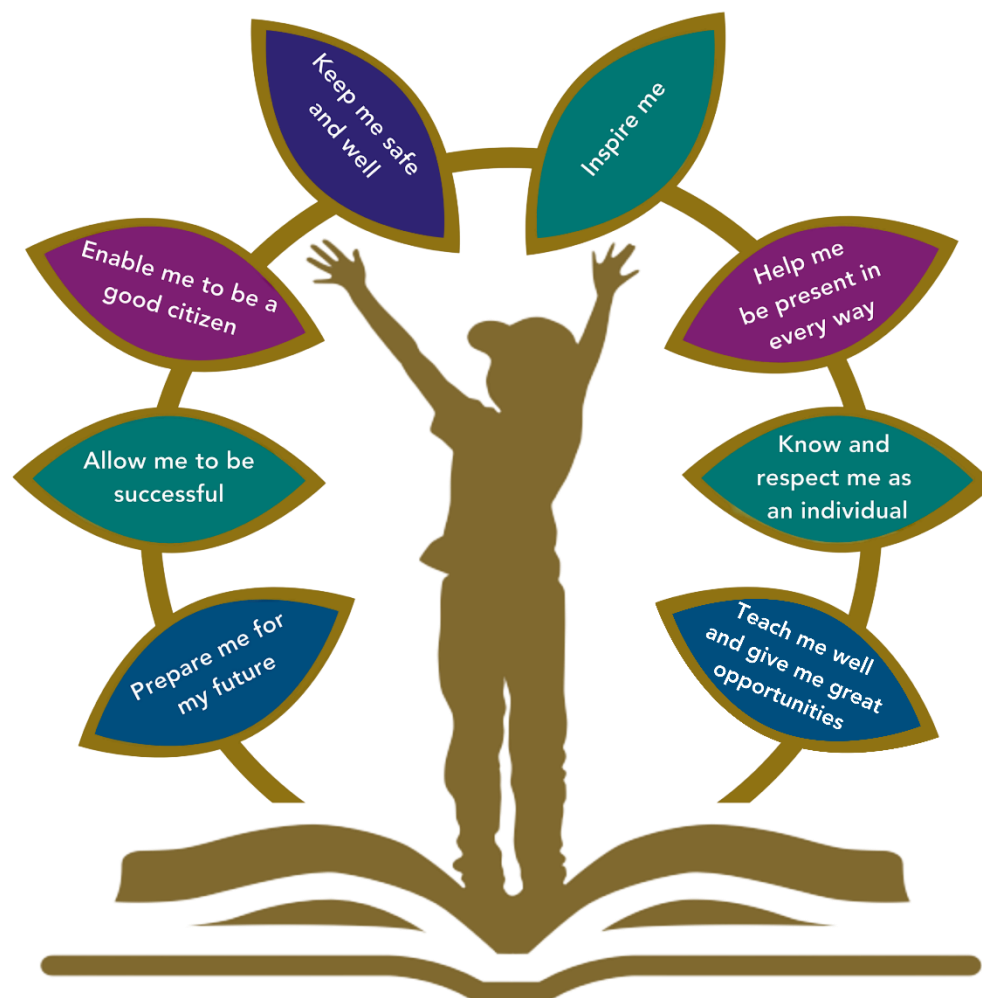
History of Policy Changes

Date	Page	Change	Origin of Change
15/08/2026	3	Added Scope	

Contents

History of Policy Changes.....	2
Contents.....	2
Introduction	3
Scope.....	3
What is Biometric Data	4
The Legal Requirements under Data Protection Act and GDPR.....	4
Consent	4
Retention of Biometric Data	5
Storage of Biometric Data	5
Appendices.....	6





Sam's Entitlement

Introduction

"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." This policy sets out to protecting the personal data of all its pupils and employees, and this includes any biometric data we collect and process.

We collect and process biometric data in accordance with relevant legislation and guidance to ensure the data and the rights of individuals are protected. This policy outlines the procedure the schools follow when collecting and processing biometric data

Scope

This policy is for all employees and pupils within a HET school or establishment (which for ease of reference are referred to throughout this document as 'schools') or the HET Managed Service (MS) Team.

What is Biometric Data

Biometric data is personal information about an individual's physical or behavioural characteristics that can be used to identify that person; this can include their fingerprints, facial shape, retina and iris patterns, and hand measurements.

All biometric data is considered to be special category data under the General Data Protection Regulation (GDPR). This means the data is more sensitive and requires more protection and this type of data could create more significant risks to a person's fundamental rights and freedoms.

A documented Data Protection Impact Assessment must be completed and approved before any biometric system is procured, piloted or implemented. The DPIA must be reviewed whenever the purpose, technology, supplier, dataset, processing method or risk profile changes, and periodically while the system remains operational.

The Legal Requirements under Data Protection Act and GDPR

'Processing' of biometric information includes obtaining, recording or holding the data or carrying out any operation or set of operations on the data including (but not limited to) disclosing it, deleting it, organising it or altering it.

As biometric data is special category data in order to lawfully process this data, HET must have a legal basis for processing personal data and a separate condition for processing special category data. When processing biometric data, HET rely on explicit consent (which satisfies the fair processing conditions for personal data and special category data). Consent is obtained using the consent form(s) in the attached appendix.

HET/School will only introduce or continue to operate a biometric recognition system where there is a clearly documented operational need and where its use is necessary, proportionate and demonstrably more appropriate than less intrusive alternatives.

Consent

HET and schools will not process any biometric data without gaining explicit consent.

Consent for Pupils

- When obtaining consent for pupils, parents will be notified that the school intend to use and process their child's biometric information. The school only require written consent from one parent (in accordance with the Protection of Freedoms Act 2012), provided no parent objects to the processing.
- If a parent objects to the processing, then the school will not be permitted to use that child's biometric data and alternatives will be provided.
- A pupil may also object to the processing of their biometric data. If a pupil objects, the school will not process or continue to process their biometric data, irrespective of whether consent has been provided by the parent(s).
- Where there is an objection, the school will provide reasonable alternatives which will allow the child to access the same facilities that they would have had access to, had their biometrics been used.
- Pupils and parents can also object at a later stage to the use of their biometric data. Should a parent wish to withdraw their consent, they can do so by writing to the school administration team requesting that the school no longer use their child's biometric data.
- The consent will last for the period that the pupil attends the school (unless it is withdrawn).



Consent for Employees

- HET/School will seek consent of employees before processing their biometric data. If the employee member objects, HET/School will not process or continue to process the biometric data and will provide reasonable alternatives.
- Employees who wish for HET/School to stop using their biometric data should do so by writing to the IT Team, via the IT Helpdesk.
- The consent will last for the period that the employee remains employed by the HET/School (unless it is withdrawn).

Retention of Biometric Data

Biometric data will be stored by the HET/School for as long as consent is provided (and not withdrawn).

Once a pupil or employee leaves, the biometric data will be deleted from the school's system no later than 15 working days.

At the point that consent is withdrawn, the school will take steps to delete their biometric data from the system no later than 15 working days after notification.

Storage of Biometric Data

Biometric data will be kept securely, and systems will be put in place to prevent any unauthorised or unlawful access/use.

The biometric data is only used for the purposes for which it was obtained, and such data will not be unlawfully disclosed to third parties.

Appendices

Use of Biometric Systems Consent Template

If the school uses biometric systems (e.g. fingerprint/palm recognition technologies) to identify children for access, attendance recording, charging, library lending, dinner systems, etc. it must (under the "Protection of Freedoms" legislation) seek permission from a parent or carer. It is also recommended that they obtain this permission through the normal internet use permission/acceptable use agreement. Schools may therefore wish to add a section such as that below to this permission form.

The school uses biometric systems for the recognition of individual children in the following ways:

- Civica (dinner system).

Biometric technologies have certain advantages over other automatic identification systems as pupils do not need to remember to bring anything with them (to the canteen or school library) so nothing can be lost, such as a swipe card.

The school has carried out a privacy impact assessment and is confident that the use of such technologies is effective and justified in a school context.

No complete images of fingerprints/palms are stored and the original image cannot be reconstructed from the data. That is, it is not possible for example, to recreate a pupil's fingerprint or even the image of a fingerprint from what is in effect a string of numbers.

Parents/Carers are asked for permission for these biometric technologies to be used by their child:

Parent/Carers Name

Pupil Name

As the parent/carers of the above pupil, I agree to the school using biometric recognition systems, as described above. I understand that the images cannot be used to create a whole fingerprint/palm print of my child and that these images will not be shared with anyone outside the school.

Yes / No

Signed

Date