



# **BRENTSIDE HIGH SCHOOL**

---

LEARNING AND ACHIEVING TOGETHER

## **Biometrics Policy**

Ratified by Governors	12 March 2025
Review date	March 2026
Staff responsible	Monica Miglior

## Table of Contents

1.	
1. Document Owner and Approval.....	3
2. Biometrics Policy.....	3
2.1 What is Biometric Data? .....	3
2.2 How does an Automated Biometric Recognition System work? .....	3
2.3 The Legal Requirements under UK GDPR.....	4
2.4 Consent and Withdrawal of Consent.....	4
<i>Consent for students</i> .....	4
2.5 Retention of Biometric Data .....	5
Appendix 1: Biometric Consent (given by parent/carer).....	6
Appendix 2 – Biometric Consent Form (staff) .....	8

## 1. Document Owner and Approval

The SBM is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the School's policy review schedule.

A current version of this document is available to all members of staff: T:\STAFF READ\General information\Policies\CURRENT.

## 2. Biometrics Policy

### 2.1 What is Biometric Data?

Biometric data means personal information about an individual's physical or behavioural characteristics that can be used to identify that person. This can be their fingerprints, facial shape, retina and iris patterns and hand measurements. Brentside High School's catering supplier uses a biometric recognition system for the processing of **finger print** biometric data, as a secure means to identify students and staff at the canteen tills.

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

This policy complies with The Protection of Freedoms Act 2012 (sections 26 to 28), the Data Protection Act 2018 and the UK GDPR.

In 2023 the School carried out a Data Protection Impact Assessment to evaluate whether the use of biometric data is a necessary and proportionate means of achieving a legitimate objective.

The result of the Data Protection Impact Assessment has informed the School's use of biometrics and the contents of this policy.

The school is operating as Data Controller.

### 2.2 How does an Automated Biometric Recognition System work?

An automated biometric recognition system uses technology which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (i.e. electronically). In order to recognise or identify an individual, information from the individual is automatically compared with biometric information stored in the system to see if there is a match.

The School does not process biometric data itself but relies on its catering supplier's biometric recognition system provider for the processing of **finger print** biometric data, as a secure means to identify students and staff at the canteen tills.

Each individual fingerprint is converted into an algorithm, which is encrypted and cannot be interpreted back into a usable fingerprint image. The solution is secure because the matching can only be done with the individual's consent, as the finger has to be presented to the scanner device for matching. Neither the School nor the system provider hold images of fingerprints in their systems.

The School or caterer cannot allow access to biometric data by anyone for any other means than for

the purpose the data was collected for, which is to identify an individual. Any biometric data that belongs to an individual that leaves the school is purged from the system.

Thumb readers ensure security, by making fraud impossible, and efficiency, as there is no need for individuals to carry money or swipe cards which can get lost or stolen. They also eliminate the risk that students entitled to free school meals be easily identifiable by their peers, thus removing any stigma associated with free-school-meal entitlement or any sense of separation.

### **2.3 The Legal Requirements under UK 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.

Biometric data is special category data, so in order to lawfully process this data, the School must have a legal basis for processing personal data and a separate condition for processing special category data. When processing biometric data, the School's caterer 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 Appendix 1.

The School process, via their caterer, biometric data to maximise security, efficiency and confidentiality for students and staff purchasing food in the school canteen.

### **2.4 Consent and Withdrawal of Consent**

The School's catering provider will not process biometric information without the relevant consent, such consent to be collected from students and staff by the School.

#### *Consent for students*

When obtaining consent for students, both parents will be notified that the School/its supplier intend to use and process their child's biometric information (as long as the school has contact details for both). 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, such as the use of a PIN.

The child may also object to the processing of their biometric data. If a child 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 for identification, such as a 4-digit PIN, which will allow the child to access the same facilities that they would have had access to had their biometrics data been used.

Students and parents can also object at a later stage to the use of their child's biometric data. Should a parent wish to withdraw their consent, they can do so by writing to the School at [info@brentsidehigh.ealing.sch.uk](mailto:info@brentsidehigh.ealing.sch.uk), requesting that the School no longer use their child's biometric data. Students who wish for the School to stop using their biometric data do not have to put this in writing but should let the school Reception know.

The consent will last for the time period that the child attends the School (unless it is withdrawn).

#### *Consent for staff*

The School will seek consent from staff before processing their biometric data. If the staff member objects, the School will not process or continue to process the biometric data and will provide reasonable alternatives such as the use of a PIN.

The consent will last for the time period that the staff member remains employed by the School, unless it is withdrawn by staff by writing to [info@brentsidehigh.ealing.sch.uk](mailto:info@brentsidehigh.ealing.sch.uk).

### **2.5 Retention of Biometric Data**

Biometric data will be stored by the school caterer's biometric processing software provider for as long as the student or member of staff remains at the school unless consent is withdrawn.

Once a student or staff member leaves, the biometric data gets deleted from the system provider's records within 72 hours.

### **2.6 Storage of Biometric Data**

At the point that consent is withdrawn, the School will take steps to delete biometric data from the system within 72 hours.

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.

## **Appendix 1: Biometric Consent (given by parent/carer)**

Biometric systems convert personal biological measurements or physical characteristics into a unique code used to identify an individual.

The school canteen uses a scanner to convert points on your child's finger/thumb into a unique biometric code, which is stored by a software provider called Civica. It is not a fingerprint in any way, shape or form and is not shared with the school or any other party. Your child's code will be automatically erased from the system when they leave Brentside High School.

When a student places their finger/thumb on the scanner, the system identifies their account and allows them to purchase food and drinks, removing the need for cash or lunch cards.

I DO give consent for my child to be registered on the school's biometric cashless catering system:

- Yes
- No

## Appendix 2: Biometric Consent Form (Staff)

Please sign below if you consent to the school taking and using your fingerprint information as part of an automated biometric recognition system.

The School's catering provider uses an automated biometric recognition system using fingerprints, which is supplied by a company called Civica.

Each individual fingerprint is converted into an algorithm, which is encrypted and cannot be interpreted back into a usable fingerprint image. The solution is secure because the matching can only be done with the individual's consent, as the finger has to be presented to the scanner device for matching. Neither the School nor the system provider hold images of fingerprints in their systems.

For staff to be able use this system, the School requires the consent in order that their biometric information can be processed. No biometric information is shared with third parties and is retained in the form of an algorithm rather than an actual fingerprint.

If a member of staff chooses not to give consent, the School will provide alternative methods of identification, such as a 4-digit PIN code, although the School's preference is always to use biometrics, as this is more secure and faster than any other method of identification.

In signing this form, you are authorising the School to use your biometric information for this purpose until you either leave the School or cease to use the system.

If you wish to withdraw your consent at any time, please do so by writing to [info@brentsidehigh.ealing.sch.uk](mailto:info@brentsidehigh.ealing.sch.uk).

**Staff Consent:**

Having read the above guidance information, I give consent to information from my fingerprint being taken and used by the school for use as part of an automated biometric recognition system.

I understand that I can withdraw this consent at any time.

Staff name: .....

Signature: .....

Date: .....

Please return a copy of this consent form to [info@brentsidehigh.ealing.sch.uk](mailto:info@brentsidehigh.ealing.sch.uk)