Last review: November 2023
Review date: November 2024
Signed By:
Approval Committee: Governing Body

GILLINGHAM SCHOOL

Hardings Lane, Gillingham

Dorset SP8 4QP

BIOMETRIC INFORMATION POLICY

Gillingham School

Biometric Information Policy

Statement of intent

Gillingham School is committed to protecting the personal data of all its students and staff; this includes any biometric data collected and processed. The School collects and processes biometric data in accordance with relevant legislation and guidance to ensure the data and the rights of individuals are protected.

This Policy operates in conjunction with the School's **Data Protection (GDPR) Policy** and **Privacy Notice.**

Why does Gillingham School process biometric data?

Biometric data, in the form of a thumbprint, is used by students to make cashless payments in the school canteen, and to enable sixth form students to sign in and out of the school site. For additional security, fingerprints are not stored as images but as encoded extracts.

The probability of two people sharing the same biometric data is virtually zero which means that an individual can be identified to a high level of accuracy. An individual's biometric data is almost impossible to replicate making it a secure means of identification, which deters and prevents fraudulent transactions and impersonation of another individual. In terms of convenience, passwords can be copied or easily forgotten, whereas the use of biometric data eliminates their use in normal operation.

Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Protection of Freedoms Act 2012
- Data Protection Act 2018
- General Data Protection Regulation (GDPR)
- Department for Education (DfE) (2018) Protection of biometric information of children in schools and colleges

Definitions

Biometric data: Personal information about an individual's physical or behavioural characteristics that can be used to identify that person, including their fingerprints, facial shape, retina and iris patterns, and hand measurements.

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

Processing biometric data: Processing biometric data includes obtaining, recording or holding the data or carrying out any operation on the data including disclosing it, deleting it, organising it or altering it. An automated biometric recognition system processes data when:

- Recording students' biometric data, e.g. taking measurements from a fingerprint via a fingerprint scanner.
- Storing students' biometric information on a database.
- Using students' biometric data as part of an electronic process, e.g. by comparing it with biometric information stored on a database to identify or recognise students.

Special category data: Personal data which the GDPR says is more sensitive, and so needs more protection – where biometric data is used for identification purposes, it is considered special category data.

Roles and responsibilities

Governing Body: Reviewing this policy on an annual basis.

Headteacher: Ensuring the provisions in this policy are implemented consistently.

The Data Protection Officer (DPO):

1) Monitoring the school's compliance with data protection legislation in relation to the use of biometric data.
2) Advising on when it is necessary to undertake a data protection impact assessment (DPIA) in relation to the school's biometric system(s).
3) Being the first point of contact for the Information Commissioner's Office (ICO) and for individuals whose data is processed by the school and connected third parties.

Data protection principles

The school processes all personal data, including biometric data, in accordance with the key principles set out in the GDPR.

The school ensures biometric data is:

- Processed lawfully, fairly and in a transparent manner.

- Only collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date, and that reasonable steps are taken to ensure inaccurate information is rectified or erased.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Processed in a manner that ensures appropriate security of the information, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Notification and consent

Where the school uses students' biometric data as part of an automated biometric recognition system (e.g. using students' fingerprints to receive school dinners instead of paying with cash), the school will comply with the requirements of the Protection of Freedoms Act 2012.

Prior to any biometric recognition system being put in place or processing a student's biometric data, the school will send the student's parents a Parental Notification and Consent Form for the use of Biometric Data.

Consent will be sought from at least one parent of the student before the school collects or uses a student's biometric data. 6.4. The name and contact details of the student's parents will be taken from the school's admission register.

Where neither parent of a student can be notified, consent will be sought from the following individuals or agencies as appropriate:

- If a student is being 'looked after' by the Local Authority (LA) or is accommodated or maintained by a voluntary organisation, the LA or voluntary organisation will be notified and their written consent obtained.
- If the above does not apply, then notification will be sent to all those caring for the student and written consent will be obtained from at least one carer before the student's biometric data can be processed.

Notification sent to parents and other appropriate individuals or agencies will include information regarding the following:

- Details about the type of biometric information to be taken.

- How the data will be used.
- The parent's and the student's right to refuse or withdraw their consent.
- The school's duty to provide reasonable alternative arrangements for those students whose information cannot be processed.

The school will not process the biometric data of a student under the age of 18 in the following circumstances:

- The student (verbally or non-verbally) objects or refuses to participate in the processing of their biometric data.
- No parent or carer has consented to the processing.
- A parent has objected in writing to such processing, even if the other parent has given written consent.

Parents and students can object to participation in the school's biometric system(s) or withdraw their consent at any time. Where this happens, any biometric data relating to the student that has already been captured will be deleted.

Where staff members or other adults use the school's biometric system(s), consent will be obtained from them before they use the system. Staff and other adults can object to taking part in the school's biometric system(s) and can withdraw their consent at any time. Where this happens, any biometric data relating to the individual that has already been captured will be deleted. Alternative arrangements will be provided to any individual that does not consent to take part in the school's biometric system(s).

<u>Alternative arrangements</u>

Parents, students, staff members and other relevant adults have the right to not take part in the school's biometric system(s).

Where an individual objects to taking part in the school's biometric system(s), reasonable alternative arrangements will be provided that allow the individual to access the relevant service, e.g. where a biometric system uses student's fingerprints to pay for school meals, the student will be able to use cash for the transaction instead. Alternative arrangements will not put the individual at any disadvantage or create difficulty in accessing the relevant service, or result in any additional burden being placed on the individual (and the student's parents, where relevant).

Data retention

Biometric data will be managed and retained in line with appropriate regulations. If an individual (or a student's parent, where relevant) withdraws their consent for their/their child's biometric data to be processed, it will be deleted from the school's system.