Hitchin Girls' School

Protection of Biometric Information Policy

This is a statutory policy required of all Academies under the Protection of Freedoms Act 2012

Date of issue:	**October 2023**
Trust Board approval:	**October 2023**
Review date:	**October 2024**

Statement of intent

Hitchin Girls' 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 outlines the procedure the school follows when collecting and processing biometric data.

1. Legal framework

1.1. 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

1.2. This policy operates in conjunction with the following school policies:

- Data Protection Policy
- Records Management and Retention Policy
- Data Security Policy and Breach Prevention and Management Plan

2. Definitions

2.1. **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.

2.2. **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.

2.3. **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.

2.4. **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.

3. Roles and responsibilities

3.1. The Board of Trustees is responsible for:

- Reviewing this policy on an annual basis.

3.2. The Headteacher is responsible for:

- Ensuring the provisions in this policy are implemented consistently.

3.3. The Data Protection Officer (DPO) is responsible for:

- Monitoring the school's compliance with data protection legislation in
- relation to the use of biometric data.
- Advising on when it is necessary to undertake a data protection impact assessment (DPIA) in relation to the school's biometric system(s).
- 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.

4. Data protection principles

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

4.2. 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.

4.3. As the data controller, the school is responsible for being able to demonstrate its compliance with the provisions outlined in 4.2.

5. Data protection impact assessments (DPIAs)

5.1. Prior to processing biometric data or implementing a system that involves processing biometric data, a DPIA will be carried out.

5.2. The DPO will oversee and monitor the process of carrying out the DPIA.

5.3. The DPIA will:

- Describe the nature, scope, context and purposes of the processing.
- Assess necessity, proportionality and compliance measures.
- Identify and assess risks to individuals.
- Identify any additional measures to mitigate those risks.

5.4. When assessing levels of risk, the likelihood and the severity of any impact on individuals will be considered.

5.5. If a high risk is identified that cannot be mitigated, the DPO will consult the ICO before the processing of the biometric data begins.

5.6. The ICO will provide the school with a written response (within eight weeks or 14 weeks in complex cases) advising whether the risks are acceptable, or whether the school needs to take further action. In some cases, the ICO may advise the school to not carry out the processing.

5.7. The school will adhere to any advice from the ICO.

6. Notification and consent

Please note that the obligation to obtain consent for the processing of biometric information of children under the age of 18 is not imposed by the Data Protection Act 2018 or the GDPR. Instead, the consent requirements for biometric information is imposed by section 26 of the Protection of Freedoms Act 2012.

6.1. 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.

6.2. 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.

6.3. Written 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.

6.5. Where the name of only one parent is included on the admissions register, the Headteacher will consider whether any reasonable steps can or should be taken to ascertain the details of the other parent

6.6. The school does not need to notify a particular parent or seek their consent if it is satisfied that:

- The parent cannot be found, e.g. their whereabouts or identity is not known.
- The parent lacks the mental capacity to object or consent.
- The welfare of the student requires that a particular parent is not contacted, e.g. where a student has been separated from an abusive parent who must not be informed of the student's whereabouts.
- It is otherwise not reasonably practicable for a particular parent to be notified or for their consent to be obtained.

6.7. Where neither parent of a student can be notified for any of the reasons set out in 6.6, 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.

6.8. 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 (see section 7).

6.9. 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 in writing to the processing.
- A parent has objected in writing to such processing, even if the other parent has given written consent.

6.10. 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.

6.11. If specific biometric data beyond student photographs is required, e.g. fingerprints, the parent will discuss this with the child and then provide or refuse consent.

6.12. Where staff members or other adults use the school's biometric system(s), consent will be obtained from them before they use the system.

6.13. 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.

6.14. Alternative arrangements will be provided to any individual that does not consent to take part in the school's biometric system(s), in line with section 7 of this policy.

7. Alternative arrangements

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

7.2. 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.

7.3. 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).

8. Data retention

8.1. Biometric data will be managed and retained in line with the school's Records Management Policy.

8.2. 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.

9. Breaches

9.1. There are appropriate and robust security measures in place to protect the biometric data held by the school. These measures are detailed in the school's Data and E-Security Breach Prevention and Management Plan.

9.2. Any breach to the school's biometric system(s) will be dealt with in accordance with the Data and E-Security Breach Prevention and Management Plan.

10. Monitoring and review

10.1. The Board of Trustees will review this policy on a bi-annual basis.

10.2. Any changes made to this policy will be communicated to all staff, parents and students.

Appendix 1

Parental Notification and Consent Form for the use of Biometric Data

Dear Parent/Carer

Cashless Catering System

We operate a cashless catering system in school which will be available for your child to use.

The system uses the latest biometric technology. This scans the student's finger, generating a unique number that is used in the system to identify your child and allow them to spend money from their cashless account. The fingerprint image is not stored and cannot be used by any other system. The system is in use in many schools around Hertfordshire and the rest of the country.

The information from your child that we wish to use is referred to as 'biometric information'. Under the Protection of Freedoms Act 2012 (sections 26 to 28), we are required to notify each parent of a child and obtain the written consent of at least one parent before being able to use a child's biometric information for an automated system. The attached sheet explains what this information is and how it is used at Hitchin Girls' School. There are also details of our legal obligations.

The process for students to register and use the system will be as follows:

1. Registration of student biometric data into the system. The student's cashless account is set up and their finger scanned to associate the student with their account.
2. Payments. Parents and carers can pay on-line via the school's ParentPay system and this is credited to the student's account.
3. Paying for items. The student chooses items from the dining room and scans their finger at the till. This displays their name, photo and account balance to the till operator who then enters the cost of their food items. The total is deducted from the account and the transaction is then complete.

In order for your child to make purchases from the school's catering facilities, we require written consent from parents to register students on the biometric system. Please complete the consent form and return it to the School to allow us to set up your child with a cashless account for the start of term.

We recommend that parents' consent is given to the new system even if their child thinks that they may not use the catering facilities to allow for changes in circumstances or occasional future use.

If any parent has questions or concerns regarding the new system, please contact the school.

Yours sincerely

Headteacher

Biometric Information – the facts (and reassurances)

Biometric information is information about a person's physical or behavioural characteristics that can be used to identify them, for example, information from their fingerprint.

This information is used as part of an automated biometric recognition system. This system will take measurements of the persons fingerprint and convert these measurements into a template to be stored on the system. An image of the fingerprint is not stored, only an encoded extract. The template (i.e. measurements taken from the fingerprint) is what will be used to activate the account.

Specific to our system – a partial image of each person's finger is uploaded and then stored in an encrypted form only on the PC running the till screens and the connected image recognition units. It does not send any information back to the school database. This partial image cannot be used for any other purpose. Usually, only the index finger of the right hand has a partial image taken, which is then converted into a number to be used for identification.

The use of the biometric system for catering purposes is sometimes confused with the use of biological material and biometric data in the criminal or terrorism context. The biometric systems in use in education do not precisely identify individuals in the general population in the way that police fingerprinting may do. The system merely distinguishes between different students well enough to charge the correct ones for their purchases. The data is not available anywhere else, it is a closed system and the data is only used in this setting. An individual's biometric data is almost impossible to replicate making it a secure means of identification.

The law places specific requirements on schools when using personal information, such as biometric information, about students for the purposes of an automated biometric recognition system.
For example:

(a) the school cannot use the information for any purpose other than those for which it was originally obtained and made known to the parents;
(b) the school must ensure that the information is stored securely;
(c) the school must tell you what it intends to do with the information;
(d) unless the law allows it, the school cannot disclose personal information to another person/body – you should note that the only persons/bodies that the school wishes to share the information with is Live Register, the system supplier. This is necessary in order to run the system.

Providing your consent/objecting
As stated above, in order to be able to use your child's biometric information, the written consent of at least one parent is required. However, consent given by one parent will be overridden if the other parent objects in writing to the use of their child's biometric information. Similarly, if your child objects to this, the school cannot collect or use her biometric information for inclusion on the automated recognition system.

You can also object to the proposed processing of your child's biometric information at a later stage or withdraw any consent you have previously given. This means that, if you give consent but later change your mind, you can withdraw this consent. Please note that any consent, withdrawal of consent or objection from a parent must be in writing.

Even if you have consented, your child can object or refuse at any time to their biometric information being taken/used. Their objection does not need to be in writing. We would appreciate it if you could discuss this with your child and explain to them that they can object to this if they wish.

The school is also happy to answer any questions you or your child may have.

If you do not wish your child's biometric information to be processed by the school, or your child objects to such processing, the law says that we must provide reasonable alternative arrangements for children who are not going to use the automated system to pay for food in the dining room. With the new catering payment system, anyone without consent can be issued with a 5 digit PIN number to be used at the till.

If you give consent to the processing of your child's biometric information, please sign, date and return the enclosed consent form to the school.

Please note that when your child leaves the school, or if for some other reason they cease to use the biometric system, their biometric data will be securely deleted.

Further information and guidance
This can be found via the following links:

Department for Education's 'Protection of biometric information of children in schools – Advice for proprietors, governing bodies, head teachers, principals and school staff': https://www.gov.uk/government/publications/protection-of-biometric-information-of-children-in-schools