HAYDON SCHOOL

Protection of Biometric Information Policy

Mission Statement

Haydon School is committed to the achievement of individual excellence, encouraging students to be creative and considerate, confident of their role in society and capable of rising to the challenges of a diverse and rapidly developing global economy.

Contents

Statement of Intent

Haydon School ('the School') is committed to protecting the personal data of our students, staff and governors; 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. We will treat the data collected with appropriate care. This Policy outlines the procedure the School follows when collecting and processing biometric data.

In common with most UK secondary schools, the School uses an electronic system for purchases from our canteen, the Pod and the Café located in the Sixth Form area. Students and staff identify themselves in the canteen, the Pod and the Café by using their fingerprint.

The cashless catering system negates the need for students and staff to carry cash and enables quick and efficient processing. Students eligible for free school meals are also no longer distinguishable from other students, therefore removing any potential awkwardness associated with their entitlement.

The system measures many aspects of the finger/thumb to do this. When a user has their finger/thumb registered, it will be translated into a unique identification code. **The system does not store an image of the finger/thumbprint and the original image cannot be reconstructed from the data stored.**

From September 2022 students' biometric information will be collected and used by the School for the administration of library loans.

The School will not use biometric information without first seeking appropriate consent.

1.Legal framework

1.1 This Policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:
- Protection of Freedoms Act 2012;
- Data Protection Act 2018 ('DPA 2018');
- The UK General Data Protection Regulation ('UK GDPR');
- DfE (2018) 'Protection of biometric information of children in schools and colleges';
- DfE (2018) 'Data protection: a toolkit for schools'.

1.2 This Policy operates in conjunction with the following policies:
- GDPR Policy;
- Records Management and Retention Policy;
- E-Safety and ICT Policy;
- Code of Conduct.

2. Definitions

2.1 **Biometric data** is personal information, resulting from specific technical processing, 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. All biometric data is personal data.

2.2 An **automated biometric recognition system** is 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. Biometric recognition systems can use many kinds of physical or behavioural characteristics, such as those listed above.

2.3 **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' and staff biometric data, e.g. taking measurements from a fingerprint via a fingerprint scanner;
- storing students' and staff biometric information on a database;
- using students' and staff 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 or staff.

2.4 **Special category data** is personal data which the UK 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 Governing Board is responsible for reviewing this Policy on an annual basis.

3.2 The Director of Finance and Operations is responsible for:

- ensuring the provisions in this Policy are implemented consistently;
- communicating any changes to this Policy to all members of staff and parents.

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 systems;
- advising on specific minimum terms designed to ensure that processing carried out by a processor meets all the UK GDPR requirements;
- being the first point of contact for the ICO and for individuals whose data is processed by the School and connected third parties.

3.4 The Network Manager is responsible for:

- ensuring that the system specifications comply with the law and best practice;
- ensuring the system is kept operational at all times;
- ensuring appropriate technical measures are in place to safeguard collected biometric information including protection against unauthorised or unlawful processing, accidental loss, destruction or damage;
- identification of systems' faults and their repair in a timely manner;
- maintenance of the School's servers on which the biometric data is kept;
- ensuring that biometric data is accurate and kept up-to-date;
- ensuring that biometric data is kept for no longer than is necessary and is destroyed in line with the Records Management and Retention Policy when it falls outside of its retention period;
- where a processor is used, the Network Manager must ensure that there is a written contract in place between the School and the processor outlining specific minimum terms designed to ensure that processing carried out by a processor meets all the UK GDPR requirements. A copy of the contact should be passed to the DPO;
- carrying out and updating the DPIA, keeping the DPIA under review.

3.5 Admissions Officer is responsible for:

- collecting biometric parental and students' consent (if applicable) at the point of registration and ensuring that a relevant Biometric Notification and Privacy Notices are available to parents and students to view. Where the name of only one parent is included on the admissions register, the Admission Officer in consultation with the Student Services Manager will consider whether any reasonable steps can or should be taken to ascertain the details of the other parent;
- recording consent on the School's MIS;
- ensuring that the consent information is passed to the DPO, relevant Year Offices and a member of staff responsible for the collection of biometric data before the processing of the biometric data begins.

3.6 The HR Manager is responsible for collecting and maintaining biometric consent for all School employees. Where staff members or other adults use the School's biometric system(s), consent will be obtained from them by the HR Manager before the processing of the biometric data begins.

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 UK 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 paragraph 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;
- be reviewed frequently and kept updated.

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. The ICO will provide the School with a written response (within eight weeks or fourteen 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. The School will adhere to any advice from the ICO.

6.Notification and consent

6.1 The obligation to obtain consent for the processing of biometric information of children under the age of 18 is not imposed by the DPA 2018 or the UK GDPR. Instead, the consent requirements for biometric information are imposed by section 26 of the Protection of Freedoms Act 2012.

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

6.3 Prior to any biometric recognition system being put in place or processing student's biometric data, the School will ask the student's parents (and the student as appropriate) for their consent for the use of Biometric Data.

6.4 Written consent (usually collected online at the point of first registration) will be sought from at least one parent of the student before the School collects or uses student's biometric data.

6.5 The name and contact details of the student's parents will be taken from the School's admission register.

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

6.7 The School does not need to notify a particular parent or seek their consent if it is satisfied that:

- othe parent cannot be found, e.g. their whereabouts or identity is not known;
- othe parent lacks the mental capacity to object or consent;
- othe 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;
- oit is otherwise not reasonably practicable for a particular parent to be notified or for their consent to be obtained.

6.8 Where neither parent of a student can be notified for any of the reasons set out above, consent will be sought from the following individuals or agencies as appropriate:

- o if a student is being 'looked after' by the LA or is accommodated or maintained by a voluntary organisation, the LA or voluntary organisation will be notified and their written consent obtained;
- o 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.

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

- o details about the type of biometric information to be taken;
- o how the data will be used;
- o how the data will be stored;
- o the parent's and the student's right to refuse or withdraw their consent;
- o the School's duty to provide reasonable alternative arrangements for those students whose information cannot be processed.

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

- o the student (verbally or non-verbally) objects or refuses to participate in the processing of their biometric data;
- o no parent or carer has consented to the processing;
- o a parent has objected in writing to such processing, even if another parent has given written consent.

6.11 Parents and students can object to participation in the School's biometric systems or withdraw their consent at any time by emailing the DPO, dpo@haydonschool.org.uk. Where this happens, any biometric data relating to the student that have already been captured will be deleted. The School will provide students with an alternative method of accessing relevant services.

6.12 If a student objects or refuses to participate, or to continue to participate, in activities that involve the processing of their biometric data, the School will ensure that the student's biometric data is not taken or used as part of a biometric recognition system, irrespective of any consent given by the student's parent(s).

6.13 The School will seek student's consent if they have sufficient maturity to exercise their data protection rights. Students will be informed that they can object or refuse to allow their biometric data to be collected and used at the point of collection by a member of staff responsible for collection of biometric data. Parents will be informed that they can object or withdraw their consent during our online registration process. Parents will also be informed of their child's right to object and will be encouraged to discuss this with their child.

6.14 Where staff members or other adults use the School's biometric systems, consent will be obtained from them before they use the system.

6.15 Staff and other adults can object to taking part in the School's biometric systems and can withdraw their consent at any time by emailing the DPO, dpo@haydonschool.org.uk. Where this happens, any biometric data relating to the individual that has already been captured will be deleted.

6.16 Alternative arrangements will be provided to any individual that does not consent to take part in the School's biometric systems, 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 systems.

7.2 Where an individual objects to taking part in the School's biometric systems, reasonable alternative arrangements will be provided that allow the individual to access the relevant service. Please contact the Finance Office for a PIN code for the canteen.

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 and Retention Policy.

8.2 Once a parent, student or a member of staff has given consent, the consent is valid until the student or staff member leaves the School, unless consent is withdrawn, which must be in writing to the DPO, dpo@haydonschool.org.uk.

8.3 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 erased from the School's system. When an individual leaves the School, access to their biometric data will be suspended and then securely deleted.

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 E-Safety and ICT Policy.

9.2 Any breach to the School's biometric systems must be reported immediately to the DPO, dpo@haydonschool.org.uk.

10.Monitoring and review

10.1 The Governing Board will review this Policy on an annual basis.

10.2 The next scheduled review date for this Policy is June 2023.

10.3 Any changes made to this Policy will be communicated to all staff, parents and students.

Document History

Date	Status	Comments
May 2020	New	New Policy – To Student committee 01.07.20. To FGB 08.07.20 for ratification. approved
June 2022	Updated	To F&P 23.06.22. To FGB 20.07.22
Next Review Date: June 2023		