SEAHAM HIGH SCHOOL

Protection of Biometric Information Policy

Contents:

Review Date	Cycle	Reviewer	Adopted	Committee
June 2025	Annually	L Hardman	June 2025	Full Governors

Protection of Biometric Information Policy

Statement of intent

Eden Learning Trust t/a Seaham High School, is committed to protecting the personal data of all its students and staff, 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 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:

- The Protection of Freedoms Act 2012
- The Data Protection Act 2018
- The UK General Data Protection Regulation (UKGDPR)
-
- DfE (2022) 'Protection of biometric information of children in schools and colleges'
- DFE (2024) 'Use of biometric data in schools and colleges'

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

- Data Protection Policy
- Disposal of Records Policy
- Data Breach Reporting Policy
- Data Protection Impact Policy & Procedures

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 governing board 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 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 six Data Protection 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 4.2 and also that any processing carried out by a third party on their behalf complies with the Data Protection Act 2018, UK GDPR and the Protection of Freedoms Act 2012

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 which will be reviewed annually, however will be a 'living' document in ensuring that appropriate measures have been taken to comply with the regulations and requirements of the UK GDPR

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 UK 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 or for the use of photocopiers), 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/carers a Consent Form for the use of Biometric Data.

6.3. Written consent will be sought from at least one parent/carer 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/carers will be taken from the school's admission register.

6.5. Where the name of only one parent/carer 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/carer.

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

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

6.7. Where neither parent/carer 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 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. We are not required to notify or seek consent from birth parents.

6.8. Notification sent to parents/carers 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/carers 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

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/carer or carer has consented in writing to the processing
- A parent/carer has objected in writing to such processing, even if another parent/carer has given written consent

6.10. Parents/carers 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 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/carer(s).

6.12. Students will be informed that they can object or refuse to allow their biometric data to be collected and used via a consent form.

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

6.14. 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.

6.15. 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/carers, 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 given a payment card to allow this to be topped up at any Paypoint shop. Students can bypass the fingerprint for the photocopying services by login in with their school account details.

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/carers, where relevant).

8. Data retention

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

8.2. If an individual (or a student's parent/carer, where relevant) withdraws their consent for their/their child's biometric data to be processed, it will be erased 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.

9.2. Any breach to the school's biometric system(s) will be dealt with in accordance with the Data Breach Procedure.

10. Monitoring and review

10.1. The governing board will review this policy on an annual basis.

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

11. Parental Notification and Consent Form for the use of Biometric Data

Dear Parent/Carer,

Seaham High School wishes to use information about your child as part of an automated (i.e. electronically operated) recognition system. This is for the for both it's cashless catering system and photocopying/printing.

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 6o 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.

Biometric and how it will be used

Biometric information is information about a person's physical or behavioral characteristics that can be used to identify them, for example, information from their fingerprint. The school would like to take and use the information from your child's fingerprint and use this information of the purpose of providing your child with use of the catering and photocopying/printing services.

For catering, this means that students are recognised at the revaluation pay points and tills by means of a scan of their thumb or finger. There are many advantages of using this system particularly that there is no need for students to carry cash or cards around school to get lost or broken (with the associated cost and inconvenience of replacing them).

Parents/carers can top up their child's catering account online through Parentpay. If you withhold consent, your child will still be able to use the cashless catering system as the member of catering staff at the till can use the look up facility at the point of service whereby your child will need to give their name at the till point instead of using their finger/thumb print in order that money may be deducted from their account as and when they purchase food.

The biometric solution does not store finger prints. When a finger or thumb is scanned for the first time, the system creates a unique algorithm from the scanned points. This data is then encrypted and serves no purpose other than identification by the cashless system or photocopying/printing service within the school.

As a parent/carer you should note that 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 that the school:

- Cannot use the information for any purpose other than those for which it was originally obtained and made known to the parent as stated above
- Must ensure that the information is stored securely
- Must tell you what the school intends to do with the information
- Unless the law allows it, cannot disclose personal information to another person/body. You should note that the only person that the school wishes to share the information with is the supplier of the biometric systems. This is necessary for your child to be able to gain access to the cashless catering and the photocopying/printing services.

The encrypted data cannot be accessed by any person within the school or by any outside third party. When a student leaves the school, all associated personal and biometric data is removed and deleted as per the school's Privacy Notice

Consent

As stated in the guidance, 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, we must not collect or use their 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 made in writing. Even if you have consented, your child can object or refuse any time to their biometric information being taken/used. Your child's objection does not need to be in writing. We would appreciate if you could discuss this with your child and explain to them that they can object to this if they wish. We are happy to answer any questions you or your child may have.

If you do not wish your child's biometric information to be processed or if you child objects to such processing, the law says that we must provide reasonable alternative arrangements for your child.

If you give consent to the processing of your child's biometric information, please sign, date and return the enclosed consent to the school. Please note that when your child leaves the school, or if for some other reason your child ceases to use the biometric system, their biometric data will be securely deleted. .

Yours sincerely

Mr G W Lumsdon
Headteacher

- -

CONSENT FORM FOR THE USE OF BIOMETRIC INFORMATION

Please complete this form if you consent to Seaham High School taking and using information from your child's fingerprint as part of an automated biometric recognition system. This biometric information will be used by Seaham High School for the purpose of the cashless catering system and the photocopying/printing service.

In signing this form, you are authorising Seaham High School to use your child's biometric information for this purpose until they leave the school or cases to use the system.

If you wish to withdraw your consent at any time, this must be done so in writing and sent to the school at the following address:

Seaham High School
Station Road
Seaham
Co. Durham
SR7 0BH

Once your child ceases to use the biometric recognition system, their biometric information will be securely deleted by the school.

Having read guidance provided to me by Seaham High School, I give consent to information from the cashless catering and the photocopying/printing service of my child:

Name of child: …… Tutor Group: ……

Being taken and used by Seaham High School for use as part of an automated biometric recognition system for the cashless catering and the photocopying/printing service

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

Name of Parent/carer: _____

Signed: _____ Date: _____