BECKFOOT TRUST

BIOMETRICS INFORMATION POLICY

V1

December 2022

CREATING REMARKABLE SCHOOLS

Table of Contents

1.0 Policy Statement

Beckfoot Trust takes its' duty to protect the personal data of all students and staff seriously, and 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.

2.0 Scope and Purpose

The purpose of this policy is to set out clearly how we meet our statutory obligation with regards to the storing of biometric data. The policy applies to the storage of all biometric data for staff, student, and visitors. All staff who are involved in storing data are trained.

The policy should be read in conjunction with the following Beckfoot Trust policies.

- GDPR Data Protection and FOI Policy

This policy has due regard to 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)
  DfE (2018) 'Protection of biometric information of children in schools and colleges'

Biometric data: Personal information about an individual's physical or behavioural characteristics that can be used to identify that person, including their eight-point identification pattern (fingerprint), 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 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 eight point identification pattern (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.

3.0 Overarching 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

As the Data Controller, the school is responsible for being able to demonstrate compliance with the provisions outlined in Section 2 (Automated biometric recognition system)

3.1 Roles and Responsibilities

The Data and Sustainability Director is responsible for:

- Reviewing this policy on an annual basis.

The Headteacher is responsible for:

- Ensuring the provisions in this policy are implemented consistently.

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

4.0 Data Privacy Impact Assessments (DPIA)

Prior to processing biometric data or implementing a system that involves processing biometric data, a DPIA will be carried out. The DPO will oversee and monitor the process of carrying out the DPIA.

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

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

The Trust will adhere to any advice from the ICO.

5.0 Notification and Consent

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 are imposed by section 26 of the Protection of Freedoms Act 2012.

1. Where the school uses students' biometric data as part of an automated biometric recognition system (e.g. using students' eight point identification pattern (fingerprint) to receive school dinners instead of paying with cash), the school will comply with the requirements of the Protection of Freedoms Act 2012.
2. Prior to any biometric recognition system being put in place or processing a student's biometric data, the school will send the students' parents a Parental Notification and Consent Form for the use of Biometric Data. (DfE exemplar at Appendix 1)
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.
4. The name and contact details of the student's parents will be taken from the school's admission register.
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. 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

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 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

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 students right to refuse or withdraw their consent
- the school's duty to provide reasonable alternative arrangements for those students whose information cannot be processed

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 another parent has given written consent

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.

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(s).

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

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.

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.

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 4 of this policy.

6.0 Alternative Arrangements

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 school's eight point identification pattern (fingerprint) 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).

7.0 Data Retention

Biometric data will be managed and retained in line with the Trust's Records Management procedures.

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.

8.0 Breaches

There are appropriate and robust security measures in place to protect the biometric data held by the school. These measures are detailed in the Trust's GDPR Policy.

Any breach to the school's biometric system(s) will be dealt with in accordance with the GDPR Policy.

Appendix 1: Parental Notification and Consent Form (DfE Example)

Notification of Intention to Process Biometric Information.

Dear Parent/Carer

Beckfoot [name of school] wishes to use information about your child as part of an automated (i.e., electronically operated) recognition system. This is for the purposes of [specify e.g. catering, library access]. The information from your child that we wish to use is referred to as 'biometric information' (see next paragraph). 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.

Biometric information and how it will be used.

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]. The school would like to take and use information from your child's [fingerprint] and use this information for the purpose of providing your child with [specify e.g. catering, library access].

The information will be used as part of an automated biometric recognition system. This system will take measurements of your child's [fingerprint] and convert these measurements into a template to be stored on the system. An image of your child's [fingerprint] is not stored. The measurements taking from your child's [fingerprint] is what will be used to permit your child to access services.

You should note that the law places specific requirements on schools and colleges 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 parent(s) as stated above

(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/college cannot disclose personal information to another person/body – you should note that the only person/body that the school wishes to share the information with is [insert any third party with which the information is to be shared e.g. X supplier of biometric systems]. This is necessary to [say why it needs to be disclosed to the third party].

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/college cannot collect or use his/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. His/her 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 access [specify e.g. catering, library].

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 he/she ceases to use the biometric system, his/her biometric data will be securely deleted.

Consent Form for the use of Biometric Information in School

Please complete this form if you consent to the school taking and using information from your child's [fingerprint] by Beckfoot [name of school] as part of an automated biometric recognition system. This biometric information will be used by the school for the purpose of accessing [catering, library access].

In signing this form, you are authorising the school to use your child's biometric information for this purpose until he/she either leaves the school/college or ceases 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:

[insert address]

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

Having read guidance provided to me by Beckfoot [name of school], I give consent to information from the [fingerprint] of my child:

[insert name of child]

being taken and used by Beckfoot [name of school] for use as part of an automated biometric recognition system for accessing [catering, library access]

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

Name of Parent:
.....

Signature:.....Date:.....

Please return this form to: [insert delivery point].