PROTECTION OF BIOMETRIC INFORMATION OF CHILDREN POLICY

October 2019

Date ratified at Trust Board:	28 November 2019
Signature of Chair:	
Date for review:	November 2020
Author/Reviewer:	Trust ICT Team

Contents

1. Preamble

This policy complies with The Protection of Freedoms Act 2012 (sections 26 to 28) and the Data Protection Act 2018.

Schools that use students' biometric data (see 2 below) must treat the data collected with appropriate care and must comply with the data protection principles as set out in the Data Protection Act 2018.

Where the data is to be used as part of an automated biometric recognition system (see 3 below), schools must also comply with the additional requirements in sections 26 to 28 of the Protection of Freedoms Act 2012.

Schools must ensure that the parent/carer of each child is informed of the intention to use the child's biometric data as part of an automated biometric recognition system.

The written consent of at least one parent must be obtained before the data is taken from the child and used (ie. 'processed' – see 4 below). This applies to all students in schools and colleges under the age of 18. In no circumstances can a child's biometric data be processed without written consent.

Schools must not process the biometric data of a student (under 18 years of age) where:

a) the child (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data
b) no parent has consented in writing to the processing
c) a parent has objected in writing to such processing, even if another parent has given written consent

Schools must provide reasonable alternative means of accessing the services to those students who will not be using an automated biometric recognition system.

2. What is biometric data/information?

Biometric data means personal information about an individual's physical or behavioural characteristics that can be used to identify that person; this can include their fingerprints, facial shape, retina and iris patterns, and hand measurements.

The Information Commissioner considers all biometric information to be personal data as defined by the Data Protection Act 2018; this means that it must be obtained, used and stored in accordance with that Act (see relevant paragraphs below).

The Protection of Freedoms Act includes provisions which relate to the use of biometric data in schools and colleges when used as part of an automated biometric recognition system. These provisions are in addition to the requirements of the Data Protection Act 1998 (see relevant section below).

3 What is an automated biometric recognition system?

An automated biometric recognition system uses technology which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (ie. 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 in section 2 above.

4 What does processing data mean?

'Processing' of biometric information includes obtaining, recording or holding the data or carrying out any operation or set of operations on the data including (but not limited to) disclosing it, deleting it, organising it or altering it. An automated biometric recognition system processes data when:

a. recording students' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner
b. storing students' biometric information on a database system; or
c. using that data as part of an electronic process, for example, by comparing it with biometric information stored on a database in order to identify or recognise students'

The Trust currently operates a cashless catering system in two of its secondary schools and uses biometrics as a means of paying for purchases. The current method used to process this data is a fingerprint scan. This is not an actual fingerprint, an image is taken using a numeric measurement and fed into an algorithm to encrypt the data. The image itself is not stored and the system is one directional meaning that it is impossible to reverse the process to create a fingerprint.

5 Security of the information

The use of the biometric system for cashless catering purposes is sometimes confused with the use of biological material and biometric data in a criminal context. The biometric systems used in education do not precisely identify individuals in the general population in the way that police fingerprinting does. The system merely

distinguishes between different students well enough to charge the correct ones for their lunch.

The data is not shared with any external agencies and is stored on a closed system. An individual's biometric data is almost impossible to replicate making it a secure and reliable means of identification. As a finger/thumb print is unique, it would be next to impossible for someone to steal someone else's biometric fingerprint. Data is not stored on the biometric scanner, so should a scanner be stolen, there is no data to retrieve or miss-use.

6 What UK law says about biometric information used in schools

UK law states that we cannot use the information for any purpose other than which we have informed parents. We have to ensure that the information is stored securely. We have to tell you what we do with the information. We cannot disclose any of this information with another person/body except for our system supplier. We have to share this information with them in order for the system to run.

7 Who is able to give consent

The Data Protection Act 2018 gives children rights over their own data when they are considered to have adequate capacity to understand. Most children will reach this level of understanding at around age 13. For this reason, in secondary schools it will often be up to the individual child to decide whether or not to provide biometric data.

Schools must notify each parent of a student under the age of 18 if they wish to take and subsequently use the child's biometric data as part of an automated biometric recognition system.

As long as the child or a parent does not object, the written consent of only one parent will be required for a school or college to process the child's biometric information. This is also the case where parents are separated or divorced but have shared parental responsibility. We only need permission from one parent to use biometric information for their child, however, if any parent withholds consent, for example if one parent agrees and one doesn't, then we cannot, by law, go ahead. Equally we cannot use the information if your child does not agree to its use.

A child does not have to object in writing but a parent's objection must be written.

The majority of students within the Trust will start using the system at the beginning of Year 7. We will therefore seek consent from parents/carers. However, a child may consent, or choose to withdraw consent, from the age of 13. Where the school considers that the child does not have the capacity, parents/carers will be asked to provide consent.

8 Length of consent

The original written consent is valid until such time as it is withdrawn. Parents (subject to the parent's objection being in writing) or the child themselves have the right to withdraw consent at any time.

We will not seek consent on an annual basis (unless there is a change to the law). If parents do not return the consent form, the Trust will automatically consider a non-return as refusal to consent and the child will not be entered onto the system.

When the student leaves the school, their biometric data will be securely removed from the school's biometric recognition system.

9 Alternative to Biometric

The school's cashless catering system allows for an alternative to biometric scanning and any student objecting to the processing of their biometric data will be issued with a PIN code or card depending on the school.

Students should be mindful that PIN codes do not have the same level of security as biometrics. It will be the child's responsibility to remember the code and keep it secure at all times and/or keep their card safe if that is the system in use at their school.

10 Further reading

Should you wish to read further then the following websites offer further guidance and information:

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

ICO guide to data protection for organisations - https://ico.org.uk/for-organisations/guide-to-data-protection/

ICO guidance on data protection for education establishments - https://ico.org.uk/for-organisations/in-your-sector/education/

If you do not have access to the internet, please contact us and we will provide a paper copy of these documents.