Biometrics Policy

March 2024

Date Approved:	**March 24**	Review Date:	**March 26**	Approved by:	**The Trust Board**

1. Key Points

Schools that use students' biometric data (see 2.1 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 the automated biometrics recognition system (see 2.2 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 each parent of a child is notified of the school's intention to use the child's biometric data (see 2.1 below) as part of an automated biometrics recognition system.

The written consent of at least one parent of a child must be obtained before the data is taken from the child and used (i.e. "processed" – see 2.3 below). This applies to all students in school under the age of 18. In no circumstances can a child's biometrics data be processed without written consent.

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

- The child (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data;
- No parent has consented in writing to the processing; or
- 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 services for those students who will not be using an automated biometric recognition system.

2. Biometric Data & Processing

What is biometric data?

Biometrics 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.

All biometric information is considered to be personal data as defined by the Data Protection Act 1998; this means it must be obtained, used and stored in accordance with that Act (please see Fareham Academy's Data Protection Policy).

The Protection of Freedoms Act 2012 includes provisions which relate to the use of biometric data in schools when used as part of an automated biometrics recognition system. These provisions are in additional to the requirements of the Data Protection Act 1998.

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" (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.

Biometrics recognition systems can use many kinds of physical or behavioural characteristics such as those listed in 1 above.

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:

- Recording students' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner;
- Storing students' biometric information on a database system; or
- Using 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.

3. **Frequently Asked Questions**

What information should schools provide to parents/students to help them decide whether to object or for parents to give their consent?

Any objection or consent by a parent must be an informed decision – as should any objection on the part of a child. Schools should take steps to ensure parents receive full information about the processing of their child's biometric data including a description of the kind of system they plan to use, the nature of the data they process, the purpose of the processing and how the data will be obtained and used. Children should be provided with information in a manner that is appropriate to their age and understanding.

What if one parent disagrees with the other?

Schools are required to notify each parent of a child whose biometric information they wish to collect/use. If one parent objects in writing, then the school will not be permitted to take or use that child's biometric data.

How will the child's right to object work in practice – must they do so in writing?

A child is not required to object in writing. An older child may be more able to say that they object to the processing of their biometric data. A younger child may show reluctance to take part in the physical process of giving the data in other ways. In either case the school will not be permitted to collect or process the data.

Are schools required to ask/tell parents before introducing an automated biometric recognition system?

Schools are not required by law to consult parents before installing an automated biometric recognition system. However, they are required to notify parents and secure consent from at least one parent before biometric data is obtained or used for the purposes of such a system. It is up to the schools to consider whether it is appropriate to consult parents and students in advance of introducing such a system.

Do schools need to renew consent every year?

No. The original written consent is valid until such time as it is withdrawn. However, it can be overridden, at any time if another parent or the child objects to the processing (subject to the parent's objection being in writing). When the student leaves the school, their biometric data will be securely removed from the school's biometric recognition system.

Do schools need to notify and obtain consent when the school introduces an additional, different type of automated biometric recognition system?

Yes, consent must be informed consent. If, for example, a school has obtained consent for a fingerprint/fingertip system for catering services and then later introduces a system for accessing library services using iris or retina scanning, then schools will have to meet the notification and consent requirements for the new system.

Can consent be withdrawn by a parent?

Parents will be able to withdraw their consent, in writing at any time. In addition, either parents will be able to object to the processing at any time but they must do so in writing.

When and how can a child object?

A child can object to the processing of their biometric data or refuse to take part at any stage i.e. before the processing takes place or at any point after his or her biometric data has been obtained and is being used as part of a biometric recognition system. If a student objects, the school mist not start to process his or her biometric data or, they are already doing this, must stop. The child does not have to object in writing.

Will consent given on entry secondary school be valid until the child leaves the school?

Yes. Consent will be valid until the child leaves the school – subject to any subsequent objection to the processing of the biometric data by the child or a written objection from a parent. If any such objection is made, the biometric data should not be processed and the school must, in accordance with the Data Protection Act, remove it from the school's system by secure deletion.

Can the school notify parents and accept consent via email?

Yes – as long as the school is satisfied that the email contact details are accurate and the consent received is genuine.

Will parents be asked for retrospective consent?

No. Any processing that has taken place prior to the provisions in the Protection of Freedoms Act coming into force will not be affected.

Does the legislation cover other technologies such as palm and iris scanning?

Yes. The legislation covers all systems that record or use physical or behavioural characteristics for the purpose of identification. This includes systems which use palm, iris or face recognition, as well as fingerprints.

Is parental notification and consent required under the Protection of Freedoms Act 2012 for the use of photographs and CCTV in schools?

No – not unless the use of photographs and CCTV is for the purposes of an automated biometric recognition system. However, schools must continue to comply with the requirements in the Data Protection Act 1998 (DPA) when using CCTV for general security purposes or when using photographs of students as part of a manual ID system or an automated system that uses barcodes to provide services to students. Depending on the activity concerned, consent may be required under the DPA before personal data is processed. The Government believes that the DPA requirements are sufficient to regulate the use of CCTV and photographs for purposes other than automated biometric recognition systems. Photo ID card systems where a student's photo is scanned automatically to provide him or her with services would come within the obligations on schools under sections 26 to 28 of the Protection of Freedoms Act 2012 as such systems fall within the definition in that Act of automated biometric recognition systems.

4. Associated Resources

DfE guidelines for schools on communicating with parents and obtaining consent:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/692116/Protection_of_Biometric_Information.pdf

ICO guidelines to data protection:

https://icosearch.ico.org.uk/s/search.html?collection=ico-meta&query=data+protection+for+education+establishments&profile=_default

British Standards Institute guide to biometrics:

https://shop.bsigroup.com/Browse-By-Subject/Biometrics/