



HILBRE HIGH SCHOOL HUMANITIES COLLEGE

BIOMETRIC DATA POLICY

Author:
Name of Committee approved:
Date ratified at Full Trustees:
Date to be reviewed:

Jane Whisker
Full Trustee
December 2022
August 2024

Biometric information processed in schools and colleges - key points:

If you use biometric data, then that data is subject to the requirements of current Data Protection legislation. In addition, if the data is to be used as part of an automated biometric recognition system, then there is an additional requirement to comply with The Protection of Freedoms Act 2012 - Sections 26 to 28. It is imperative that schools and colleges ensure that each parent/legal guardian of a student is notified of the school's intention to use the student's biometric data as part of an automated biometric recognition system. There is no legal basis in law to rely on when using such a system in schools or colleges BUT you can seek and rely on consent.

The written consent of at least one parent/legal guardian is required before the data is taken from the student and processed. This applies to all students under the age of 18; **in no circumstances** can a student's biometric data be processed without this written consent.

Schools and colleges must not process 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/legal guardian has consented in writing to the processing; or
- c) a parent/legal guardian has objected in writing to such processing, even if another parent/legal guardian has given written consent.

Schools and colleges must provide reasonable alternative means of accessing services for those students who will not be using an automated biometric recognition system. The common use of such a system is in relation to school meal provision and library provision but there are other school services and activities which rely on biometrics.

Definition of biometric data:

Biometric data is personal information about an individual's physical or behavioural characteristics that can be used to identify that person. Commonly used biometric data are fingerprints, facial shape, retina and iris patterns, and hand measurements.

The Information Commissioner (ICO) regulates how personal data is processed and the ICO considers all biometric information to be personal data as defined by the Data Protection Act 2018 (DPA).

The Protection of Freedoms Act 2012 includes provisions which relate to the use of biometric data when it is used as part of an automated biometric recognition system. Please note these provisions are in addition to the requirements of the DPA.

What is an automated biometric recognition system?

An automated biometric recognition system uses technology to measure 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.

This automatic recognition may be used for school meals provision, for example, or when using library services in schools.

What does “processing” mean?

Processing has a wide meaning and includes obtaining, using, storing, disclosing and deleting data. Some examples of automated biometric recognition system processes data are:

1. recording student’s biometric data by taking measurements from a fingerprint via a fingerprint scanner;
2. storing students biometric information on a database system; or
3. 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.

Frequently Asked Questions:

1. What information should schools provide to parents/legal guardians/students to assist them in deciding to object/consent to biometric data being processed?

Any objection/consent must be an informed decision. Schools and colleges should take steps to ensure they provide full information about the processing of students’ biometric data. Good practice is to include this information in the school’s Privacy notice

2. What if one parent/legal guardian disagrees with the other?

Schools and colleges will be required to notify each parent/legal guardian of a student whose biometric information they wish to collect/use. If one objects in writing, then the school or college will not be permitted to take or use that biometric data. This relates to parents/legal guardians with parental responsibility in law.

3. Are schools required to consult with parents/legal guardians before introducing an automated biometric recognition system?

There is no legal requirement to consult but there is a requirement to notify and obtain consent from at least one parent/legal guardian before biometric data is obtained or processed.

4. Do schools need to seek 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 a parent/legal guardian objects to the processing in writing.

5. Do schools need to notify and obtain consent if they introduce an additional, different type of automated biometric recognition system?

Yes, you may have obtained consent for a fingerprint system for catering services and then introduce a system for accessing library services using iris or retina scanning. Consent for the new system will need to be sought.

6. Can consent be withdrawn by a parent or legal guardian?

Consent can be withdrawn at any time, in writing; this includes email if you are satisfied the contact details are accurate.

7. Is consent valid until the student leaves that school?

Yes, subject to any subsequent objection to the processing by the student or a written objection from a parent or legal guardian.

Additional guidance and advice:

DfE guidelines on biometric data in schools and colleges:

<https://www.gov.uk/government/publications/protection-of-biometric-information-of-children-in-schools>

ICO guidance for the public on personal data held by education establishments:

<https://ico.org.uk/your-data-matters/schools/>

British Standards Institute guide to biometrics:

<http://shop.bsigroup.com/en/Browse-by-Subject/Biometrics/?t=r>

For any additional information or if you have any questions or queries regarding the content of this document, please contact:

Jane Corrin at Schoolsdpo@wirral.gov.uk

Review due: August 2024