

BIOMETRIC DATA POLICY

Document Owner	James Sanford
Committee	FGB
Frequency of Review	Every 2 years
Date of last review	May 2022
Date approved by Governors	20 th September 23
Signed	<i>J. Owens</i>
Date of next review	Sept 2024

Policy statement on equality and diversity

The School will promote equality of opportunity for students and staff from all social, cultural and economic backgrounds and ensure freedom from discrimination on the basis of disability, gender, race, age, religion or belief, and sexual orientation.

Equality and diversity are integral to the School's priorities and objectives. We will support inter-faith and inter-cultural understanding and engage all students in playing a full and active role in wider engagement with society.

biometric Information processed in Schools and Colleges - Key Points

Schools and Colleges which use pupils' biometric data must treat that data in accordance with The Data Protection Act 2018; this includes the requirements of The General Data Protection Regulation (GDPR). If the data are to be used as part of an automated biometric recognition system, then Schools and Colleges must also comply with the additional requirements contained within The Protection of Freedoms Act 2012. (The relevant sections of the legislation are sections 26 to 28.)

Schools and Colleges must ensure that each parent/carer of a child is notified of the school's intention to use the child's biometric data as part of an automated biometric recognition system. The written consent of at least one parent/carer must be obtained before the data are taken from the child and processed. This applies to all pupils in Schools and Colleges under the age of 18. In no circumstances can a child's biometric data be processed without this written consent.

Schools and Colleges must not process the biometric data of a pupil who is 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/carer has consented in writing to the processing; or
- c) A parent/carer has objected in writing to such processing, even if another parent/carer has given written consent.

Schools and Colleges must provide reasonable alternative means of accessing services for those pupils who will not be using an automated biometric recognition system.

Any Biometric data held by a School or College will be deleted when a pupil leaves that educational establishment.

Biometric Data & Processing

What is biometric data?

Biometric data is simply defined as personal information about an individual's physical or behavioural characteristics that can be used to identify that person. This commonly includes 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). This means that how this data is collected, used, stored, disclosed and deleted, must be in line with the requirements of the DPA.

The Protection of Freedoms Act 2012 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 DPA.

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.

What does "processing" mean?

Processing of biometric information includes obtaining, using, storing, disclosing and deleting that data. Examples of how an automated biometric recognition system processes data are:

- a. Recording pupils' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner.
- b. Storing pupils' 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 pupils.

Frequently Asked Questions

1. What information should schools provide to parents/carers and pupils to help them decide whether to object/consent to biometric data being processed?

Any objection/consent by a parent/carer must be an informed decision. Schools and Colleges should take steps to ensure they provide full information about the processing of pupils' biometric data. This can simply be done by including it in the school's privacy notice.

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

Schools and Colleges will be required to notify each parent/carer of a child 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 child's biometric data.

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

Schools and Colleges are not required by law to consult before installing an automated biometric recognition system. However, they are required to notify and obtain consent from at least one parent/carer before biometric data is obtained or processed. Each school should consider whether it is appropriate to consult in advance of introducing such a system.

4. 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).

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

Yes, A School or College may have obtained consent for a fingerprint system for catering services and then later introduces a system for accessing library services using iris or retina scanning. New consent for the new system will need to be sought.

6. Can consent be withdrawn by a parent or carer?

Consent can be withdrawn at any time, in writing. Writing includes the use of email if the School or College is satisfied the contact details are accurate.

7. Will consent be valid until the child leaves that 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 or carer.

8. Will schools automatically delete biometric data when child leaves school or if one/both parent(s) withdraw consent?

Yes, a pupil's biometric data is deleted on leaving or if consent is withdrawn.

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 guide to data protection:

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

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:

DPO@wirral.gov.uk