JFS Policies **– Protection of Biometric Information – July 2023**

Headteacher	Chair of Governing Board
	
Dr David Moody	Mr Andrew Moss

Published Date	Staff	Review Date
July 2023	Dr David Moody	January 2025

1. Aims

Schools have a legal duty if they wish to use biometric information about students for the purposes of using automated biometric recognition systems. The duties on schools in the Protection of Freedoms Act 2012 set out in this advice came into effect from 1 September 2013.

Schools using automated biometric recognition systems, or planning to install them, should make arrangements to notify parents and obtain the consent required under the duties set out in the body of this advice. There are no circumstances in which a school or college can lawfully process a student's biometric data without having notified each parent of a child and received the necessary consent.

This advice relates to the following legislation:

- The Protection of Freedoms Act 2012
- The Data Protection Act 2018

2. Key Points

- Schools that use students' biometric data 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 used as part of an automated biometric recognition system, schools must also comply with the additional requirements in sections 26 to 28 of the Protection of Freedoms Act 2012 (see relevant section below).
- Schools must ensure that each parent 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 must be obtained before the data is taken from the child and used (i.e. 'processed'). This applies to all students in schools 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:
    - 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
    - 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.

3. What is Biometric Data?

Biometric data means personal information about an individual's physical 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 data is considered to be special category data under the UK General Data Protection Regulation (UK GDPR). This means the data is more sensitive and requires more protection as this type of data could create more significant risks to a person's fundamental rights and freedoms.

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

4. 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.

5. The Legal Requirements under UK GDPR

'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.

As biometric data is special category data, in order to lawfully process this data, the School must have a legal basis for processing personal data and a separate condition for processing special category data. When processing biometric data, the School rely on explicit consent (which satisfies the fair processing conditions for personal data and special category data).

6. Consent and Withdrawal of Consent

JFS is not currently using biometric information

6.1 Consent for Students

When obtaining consent for students, both parents will be notified that the school intends to use and process their child's biometric information. The school only requires written consent from one parent (in accordance with the Protection of Freedoms Act 2012), provided no parent objects to the processing.

If a parent objects to the processing, then the school will not be permitted to use that child's biometric data and alternatives will be provided.

The child may also object to the processing of their biometric data. If a child objects, the school will not process or continue to process their biometric data, irrespective of whether consent has been provided by the parent(s).

Where there is an objection, the school will provide reasonable alternatives which will allow the child to access the same facilities that they would have had access to had their biometrics been used.

Students and parents can also object at a later stage to the use of their child's/their biometric data. Should a parent wish to withdraw their consent, they can do so by writing to JFS.

Students who wish for the school to stop using their biometric data do not have to put this in writing but should let a member of the Senior Leadership Team know.

6.2 Consent for Staff

The School will seek consent of staff before processing their biometric data. If a staff member objects, the school will not process or continue to process the biometric data and will provide reasonable alternatives. Staff who wish for the school to stop using their biometric data should do so by writing to the Headteacher.

The consent will last for the time period that the staff member remains employed by the School (unless it is withdrawn).

7. Retention of Biometric Data

Biometric data will be stored by the school for as long as consent is provided (and not withdrawn).
Once a student or staff member leaves, the biometric data will be deleted from the school's system no later than 72 hours.

8. Storage of Biometric Data

At the point that consent is withdrawn, the School will take steps to delete their biometric data from the system and no later than 72 hours.

Biometric data will be kept securely and systems will be put in place to prevent any unauthorised or unlawful access/use.

The biometric data is only used for the purposes for which it was obtained and such data will not be unlawfully disclosed to third parties.