



The John Fisher School

Biometrics Policy

Responsible: Full Governing Board

Next Review Date: September 2023

What is Biometric Data?

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.

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 additional 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.

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.

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). Consent is obtained using the school's consent form.

The school process biometric data as an aim to make significant improvements to our canteen and lunch facilities. This is to ensure efficiency and to do away with the need for cash being used, to safeguard the students.

Consent and Withdrawal of Consent

The school will not process biometric information without the relevant consent.

Consent for pupils

When obtaining consent for students, parents/carers 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/carer (in accordance with the Protection of Freedoms Act 2012), provided no parent/carer objects to the processing.

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

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

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

Students and parents/carers can also object at a later stage to the use of their child's/their biometric data. Should a parent/carer wish to withdraw their consent, they can do so by writing to the school at johnfisherschool.org requesting that the school no longer use their child's biometric data.

Students who wish for the school to stop using their biometric data do not have to put this in writing but should let the School Business Manager know.

The consent will last for the time period that your child attends the school (unless it is withdrawn).

Consent for staff

The school will seek consent of staff before processing their biometric data. If the 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 School Business Manager.

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

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.

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.