



Statement on Biometric Recognition Systems

Summary of changes

This statement has been updated to reference data protection law. It has been adapted from the Data Protection Officer Hub standard document. V.4 has an added statement at the end regarding the associated DPIA.

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

As a data controller we will meet the requirements of the UK's data protection laws (Data Protection Act 2018 and UK GDPR) when we are using biometric data.

We will ensure that biometric data is processed lawfully, fairly and in a transparent way, and that we comply with all the GDPR principles.

All biometric data is classified as special category data under the UK GDPR which means that it merits specific protection due to its sensitivity.

Where biometric data is used as part of an automated biometric recognition system, e.g., cashless catering or photo ID card systems, we will comply with the additional requirements of the Protection of Freedoms Act 2012 (sections 26 - 28). The school will:

- ensure that each parent* is notified of the school intention to use their child's biometric data as part of an automated biometric recognition system
- ensure the written consent of at least one parent is obtained for all pupils under the age of 18 before the data is taken from the pupil and used
- not process the biometric data of a pupil (under the age of 18) where:
 - the pupil objects or refuses to participate in the processing of their biometric data (their objection or refusal can be verbal; it does not have to be in writing)
 - no parent has consented in writing to the processing (this must be a written consent)
 - a parent has objected in writing even if another parent has given their consent.

Parents and pupils can change their minds and withdraw consent at any time. We will make sure that any biometric data already captured is deleted.

We will provide alternative means of accessing services for those pupils who are not using an automated biometric system, e.g., pupils can pay for school meals in cash.

When notifying parents about the intention to take and use their child's biometric information as part of an automated biometric system, we will include:

- details about the type of biometric data to be taken
- how it will be used

Author	CEO	Approved by	Compliance
Date Approved/Reviewed	29/03/2024	Review Cycle	Yearly
Version	4	Page	Page 1 of 2

- the parents' and pupil's right to refuse or withdraw their consent at any time.
- our duty to provide reasonable alternative arrangements for those pupils who will not be using the automated biometric system.

**"parents" includes not only the biological mother or father (or the adoptive parents) but any individual with parental responsibility for the child, as set out in Part 1 of the Children Act 1989.*

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it and provide alternative means of accessing the relevant service if they object or withdraw their consent. Consent can be withdrawn at any time and any biometric data already held will be deleted.

The Data Protection Impact Assessment (DPIA) associated with the use of biometric data is reviewed annually and re-written if there are substantial changes required.

Author	CEO	Approved by	Compliance
Date Approved/Reviewed	29/03/2024	Review Cycle	Yearly
Version	4	Page	Page 2 of 2