Protection of Biometric Information Policy

Mission Statement

WeST holds a deep-seated belief in education and lifelong learning. Effective collaboration, mutual support and professional challenge will underpin our quest to ensure that all children and adults that we serve are given every opportunity to fulfil their potential and succeed in life.

Please see Annex A for details of the WeST schools that use Biometric systems.

Person(s) responsible for updating the policy:	June Smart & Judicium (DPO) ELT: Nat Parnell
Policy type:	Trust wide
Approval level:	Audit and Risk Committee
Date approved:	24 April 2025
Review frequency:	Annually
Date of next review:	April 2026

Contents

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.

- 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 from at least one parent.

- 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 or behavioural characteristics that can be used to identify that person; this can include their fingerprints, facial mapping, retina and iris patterns, facial and hand measurements. All biometric data is special category data under the UK General Data Protection Regulation (UK GDPR). This means the data is more sensitive and requires increased 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.

The individual school has carried out a Data Protection Impact Assessment with a view to evaluating whether the use of biometric data is a necessary and proportionate means of achieving the legitimate objectives set out by the school.

The result of the Data Protection Impact Assessment has informed the agreed use of biometrics and is in line with the contents of this policy.

3.1 What is Facial Recognition Technology (FRT)

Facial recognition technology relies on the use of people's personal data. Data protection law therefore applies to any organisation using it. It is a process by which a person can be identified or otherwise recognised from a digital image.

4. What is an Automated Biometric Recognition System?

An automated biometric recognition system uses technology which measures an individual's physical, behavioural or facial 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.

4.1 Facial Recognition Systems

Cameras are used to capture these images and FRT software produces a biometric template. Often, the system will then estimate the degree of similarity between two facial templates to identify a match.

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 or updating it.

As biometric data is special category data, in order to lawfully process this data, WeST schools must have a legal basis for processing personal data and a separate condition for processing special category data. When processing biometric data, WeST schools rely on explicit consent (which satisfies the fair processing conditions for personal data and special category data). Written consent can be obtained using the most appropriate method which will depend on the individual school.

Individual schools will process biometric data to make significant improvements to canteen and lunch facilities for students and staff. This is to ensure efficiency, reduce queues, to do away with the need for swipe cards and remove the requirement for cash handling in schools.

6. Consent and Withdrawal of Consent

Individual WeST schools will not process biometric information without the relevant consent. Consent can be withdrawn at any time.

6.1 Consent for Students

When obtaining consent for students, any person with parental responsibility will be notified that the individual 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, the individual 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 individual 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 individual 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 the School SIMS Administrator and requesting that the individual school no longer use their child's biometric data.

Students who wish for the individual school to stop using their biometric data do not have to put this in writing but should let the School SIMS Administrator know as soon as possible.

6.2 Consent for Staff

The individual school will seek consent of staff before processing their biometric data. If a staff member does not provide consent, the school will not process any biometric data and will provide reasonable alternatives. Staff that have previously provided consent who wish for the individual school to stop using their biometric data should do so by writing to the School SIMS Administrator / School IT Network Manager.

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

7. Retention of Biometric Data

Biometric data will be stored on individual school systems for as long as consent is provided (and not withdrawn). Once a student or staff member leaves or on removal of consent, the biometric data will be deleted from the individual school's system, this should be within 72 working hours.

8. Storage of Biometric Data

At the point that consent is withdrawn, the individual school will take steps to delete their biometric data from the system this should be with 72 working 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.

9. Annex A

Westcountry Schools Trust: Schools and organisations using Biometric Systems

Links to each schools website can be found at: WeST - Home page

Westcountry Schools Trust Member	Site Address	Biometric System Used
Callington Community College	Launceston Road, Callington, Cornwall. PL17 7DR	Fingerprint Recognition
Coombe Dean School	Charnhill Way, Elburton, Plymouth. PL9 8ES	Fingerprint Recognition
Eggbuckland Community College	Westcott Close, Eggbuckland, Plymouth. PL6 5YB	Fingerprint Recognition
Hele's School	Seymour Road, Plympton, Plymouth. PL7 4LT	Fingerprint Recognition
Ivybridge Community College	Harford Road, Ivybridge, Devon. PL21 0JA	Facial Recognition
Plymstock School	Church Road, Plymstock, Plymouth. PL9 9AZ	Facial Recognition
Sir James Smith School	Dark Lane, Camelford, Cornwall, PL32 9UJ	Fingerprint Recognition
South Dartmoor Community College	Balland Lane, Ashburton TQ13 7EW	Fingerprint Recognition

Correct as of March 2025