



Osborne
Co-operative Academy Trust

Self-help
Self-responsibility
Equity
Equality
Democracy
Solidarity

Biometrics Policy

First approved by Trust Board: September 2020

Review Frequency: Annually

Date of last review: September 2020

Date of next review: September 2021

Author/Reviewer	Date Created	Version	Notes
IGS	July 2018	1.0	Approved by Trust Board 17/9/2020

Osborne Co-operative Academy Trust is a multi-academy trust (MAT) incorporated around the principles and values of the international co-operative movement. These are Equality, Equity, Democracy, Self-help, Self-Responsibility and Solidarity, along with the ethical values of openness, honesty, social responsibility and caring for others. These values and principles underpin all our actions.

Responsibilities for the collection and management of biometric information. A biometric recognition system obtains or records information about a person's physical or behavioural characteristics and compares that information with information which has been previously stored to determine whether the person is recognised by the system.

Policy points are numbered. The numbering corresponds to explanations of 'why?' and 'how?' for each point further down the page.

What must we do?

1. **MUST:** Schools must refer to their use of biometric data in their privacy notices, ensuring individuals are clear about their rights in relation to its use
2. **MUST:** Schools must ensure that all students understand that they can object or refuse to allow their biometric data to be taken/used
3. **MUST:** Schools must **gain consent** in writing from at least one parent. Consent is **not** required from the student, even if they are aged 12 or over (but see point 9)
4. **MUST:** Schools must **document** that consent has been given
5. **MUST:** Schools must provide a simple process to **object** and **withdraw consent**
6. **MUST:** Schools must **document** if consent is withdrawn or objections are raised
7. **MUST NOT:** Schools must not continue to hold or use biometric data where consent for its use has been withdrawn
8. **MUST:** If any parent/guardian/carer withdraws consent schools must cease to hold and use the biometric data even if the other parent/guardian/carer has not withdrawn consent
9. **MUST:** Schools must accept the view of the **student** if they do not want their biometric data used by the school, regardless of their age. The student's wishes supersede any parent/guardian/carer wishes. If both or either parent has consented and the student does not wish the data to be processed, the student's wishes take precedent.
10. **MUST:** Schools must ensure that there is an **alternative arrangement** available for any services which use biometrics
11. **MUST:** Ensure that biometric data is held in an encrypted form, and that all available technical and organisational **security** measures are applied
12. **MUST:** Schools must complete a **Data Protection Impact Assessment** for the use of biometric data
13. **MUST:** Use of biometric data must be recorded in a school's **records of processing activities** (Framework document H1)
14. **MUST NOT:** Schools must not share biometric data with 3rd parties unless there is an appropriate contract in place protecting the rights of data subjects

Why must we do it?

1. The law requires us to process personal data fairly, lawfully and transparently. This means we must tell people how we use biometric data and their rights in relation to its use.
2. To comply with our legal obligations and DfE Guidance.
3. Due to the sensitivity of biometric data the only appropriate legal basis is consent from the parent/guardian/carer.
4. Data protection legislation requires consent to be evidential, and this is best achieved by gaining consent in writing.
5. Schools must have a consent withdrawal process in place which staff are aware of. Withdrawal of consent must be a simple process and must not be more difficult than the process for giving consent.
6. Schools must be able to evidence when they stopped using the data and why.
7. It is unlawful to continue to process data where consent has been withdrawn.
8. A singular parent/guardian/carer withdrawal overrides multiple consents for the same biometric data.
9. The student's wish would supersede those of either or both parent/guardian/carers.

10. Any services which use biometric recognition must have an alternative method of access to ensure equality of opportunity as this processing is consensual.
11. Biometric data is subject to a higher requirement for security because it is classed as special category data within the Data Protection Act 2018.
12. As biometric data is a special category data and is used to monitor the activities of students in certain circumstances you are required to complete a Data Protection Impact Assessment.
13. Records of Processing Activity are a legal requirement under the UK General Data Protection Act 2016 as applied by the Data Protection Act 2018.
14. To comply with the Data Protection Act 2018.

How must we do it?

1. Ensure the Biometric privacy notice provided by IGS is published on the school's website.
2. Take account of the students' age and level of understanding. Parents should also be told of their child's right to object or to refuse and be encouraged to discuss this with their child.
3. Gain consent from parents by asking them to sign a consent form which can be retained on the student file.
4. Use a consent form to gain consent from parent/guardian/carers which can be placed in the student file to evidence consent was provided. Ensure consent is requested using clear, plain language and that the parent/guardian/carer takes a positive action by ticking and signing the form, to evidence consent was given. Consent can be gained for several things on one form, however each processing activity consent is required for must be itemised to ensure that consent is sought for each activity individually within the form.
5. Schools must explain on their privacy notices and consent forms how individuals can withdraw consent or object to their use of biometric data.
6. If consent is withdrawn, or biometric processing is objected to, schools must keep a record of this in the student file which shows the actions taken to resolve matters.
7. Schools must delete the biometric data when consent for its use has been withdrawn. They must ensure that if their biometrics system is provided by a third party and includes access to biometric data that they too delete any copies of the biometric data from their systems. This should be stated in the school's contract with the 3rd party if they will have copies of the biometric data.
8. Where more than one parent/guardian/carer has consented to biometric processing, only one of those parent/guardian/carers needs to withdraw consent in order to stop the processing.
9. A student's request to stop processing their biometric data overrides that of any parent/guardian/carer and must be acted on immediately.
10. Consider the continuation of the school's previous process as an alternative to biometric recognition.
11. The data must be fully encrypted to a high level at rest and in transit and all other relevant physical or technical controls must be applied. All relevant security measures employed by the school must be applied to biometric data.
12. A Data Protection Impact Assessment is required when processing biometric data due to its sensitivity. Please seek support from IGS who can assist in this activity.
13. A school's Records of Processing Activity is provided in the IGS Framework, document ref H1. This must be maintained and regularly reviewed to meet legal obligations under the UK GDPR.
14. If a school contracts in a supplier of biometric recognition systems they must ensure that their contract with them is GDPR compliant, and that they can provide sufficient assurances of their suitability for processing such sensitive data.

Document Control

Version: **1**

Date approved: **September 2020**

Approved by: **Osborne Co-operative Academy Trust Board**

Next review: **September 2021, Annual Review**

References

- Data Protection Act 2018
- General Data Protection Regulations 2016
- Article 8, The Human Rights Act 1998
- Protection of Freedoms Act 2012
- DfE - Protection of biometric information of children in schools and colleges – March 2018



Protection_of_Biometric_Information.pdf

Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.