Approved:	September 2023
Review Date:	September 2024

POLICY DOCUMENT

Biometric Policy

ST JOHN BOSCO CATHOLIC ACADEMY

1. Introduction

1.1 What is Biometric Data?

Biometric data means personal information resulting from specific technical processing relating to the individual's physical, psychological or behavioural characteristics which allow or confirm the unique identification of that person, such as facial images, voice recognition or fingerprints.

Schools and academies that use pupils' biometric data must treat the data collected with appropriate care and must comply with the data protection principles as set out in the General Data Protection Regulation 2018.

The Information Commissioner considers all biometric information to be personal data as defined by the General Data Protection Regulation 2018; this means that it must be obtained, used and stored in accordance with the Regulation.

Personal data used as part of an automated biometric recognition system must also comply with the additional requirements in sections 26 to 28 of the Protection of Freedoms Act 2012.

The Protection of Freedoms Act 2012 includes provisions which relate to the use of biometric data in schools, academies and colleges when used as part of an automated biometric recognition system.

Schools and academies must ensure that the parent/carer of each pupil is informed of the intention to use the pupil's biometric data as part of an automated biometric recognition system. Parents/carers must be advised that alternative methods to biometric scanning are available for processing identity if required.

The written consent of the parent/carer or the pupil, where the pupil is deemed to have the capacity to consent, must be obtained before the data is taken from the pupil and processed within the biometric recognition system. In no circumstances can a pupil's biometric data be processed without written consent.

Schools and academies must not process the biometric data of a pupil where:

a) the pupil (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data;

b) a parent or pupil has not consented in writing to the processing; or

c) a parent or pupil has objected in writing to such processing, even if another parent has given written consent.

Schools and academies must provide reasonable alternative means of accessing the services to those pupils who will not be using an automated biometric recognition system.

2. Biometric Data and Processing

2.1 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). Biometric systems usually store measurements taken from a person's physical/behavioural characteristics and not images of the characteristics themselves.

2.2 What Does Processing Data Mean?

'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. An automated biometric recognition system processes data when:

a) recording pupils' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner;

b) storing pupils' biometric information on a database system;

c) using that data as part of an electronic process, for example, by comparing it with biometric information stored on a database in order to identify or recognise pupils.

It is the responsibility of the data controller to identify the additional risks associated with using automated biometric technology by conducting a DPIA ensuring decisions are documented. Controllers should also, be aware of the wider duties placed on them, for example under the Human Rights Act 1998 and Public Sector Equality Act Duty using automated biometric technology. Controllers should also consult with the ICO when making these decisions.

2.3 Who Is Able to Give Consent?

In order to comply with the requirements of the Protection of Freedoms Act 2012, the academy must notify each parent, carer/legal guardian of the child of their intention to process the child's biometric information, and that the parent may object at any time to the processing of the information. It is important to understand that a child's biometric information must not be processed unless at least one parent of the child consents, and no parent of the child has withdrawn his or her consent, or otherwise objected, to the information being processed. In

addition, a pupil's or student's objection or refusal, overrides any parental consent to the processing, therefore any biometric data must not be processed.

The Protection of Freedoms Act 2012 defines a parent to mean "a parent of the child and any individual who is not a parent of the child but who has parental responsibility for the child". Practically it would be person(s) with parental responsibility for the child, be it birth, adoptive or an appointed body, who the academy would notify and seek consent from to process personal biometric data. Any one parent could give or withhold consent.

Where a child is looked after and is subject to a care order in favour of the local authority or the local authority provides accommodation for the child within the definition of section 22(1) of the Children Act 1989, the academy would not be required to notify or seek consent from birth parents.

If a pupil or student under 18 objects or refuses to participate (or to continue to participate) in activities that involve the processing of their biometric data, the academy must ensure that the pupil/student's biometric data is not taken/used as part of a biometric recognition system. A pupil's or student's objection or refusal overrides any parental consent to the processing. Section 26 and Section 27 of the Protection of Freedoms Act 2012 makes no reference to a lower age limit in terms of a child's right to refuse to participate in sharing their biometric data.

Academies should also take steps to ensure that pupils and students understand that they can object or refuse to allow their biometric data to be taken/used and that, if they do this, the school or college must provide them with an alternative method of accessing relevant services. The steps taken by academies to inform pupils and students should take account of their age and level of understanding. Parents should also be told of their child's right to object or refuse and be encouraged to discuss this with their child.4

Once a student is 18 years old they will be considered an adult and as such parental consent is no longer relevant.

2.4 Alternative to Biometric

The academy will provide an alternative to biometric scanning for any parent/pupil objecting to the processing of biometric data.

2.5 Length of Consent

The original written consent is valid until such time as it is withdrawn. However, it can be overridden, at any time either parent/carer or the pupil themselves objects to the processing (subject to the parent's/carer's objection being in writing). When the student leaves the school or academy, their biometric data will be securely removed from the academy's biometric recognition system.

3. Monitoring and Review of This Policy

The Governing Body or Trustees shall be responsible for reviewing this policy from time to time to ensure that it meets legal requirements and reflects best practice.