The Collegiate Trust
Exceptional Education for All

BIOMETRIC DATA POLICY

Lead	Governance and Compliance Manager
Approved by TCT	November 2023
Next Review	July 2025

1. Introduction

*The Collegiate Trust (*hereafter referred to as *TCT* or *the Trust* and always meaning the Trust collectively and each school within the Trust*)* is a partnership of schools in Crawley and Croydon whose mission is *collaboration to deliver exceptional education*, and whose vision is *exceptional education for all*. This is reflected in our Trust's values: ambition & collaboration, as well as in our desired outcomes: achievement & enjoyment.

2. Purpose

In line with the purpose limitation principle under Data Protection law, schools and colleges can only store and use the biometric information for the purpose for which it was originally obtained and parental/child consent given.

3. What is Biometric Data

3.1 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.

3.2 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

3.3 The decision to use automated biometric technology rests with individual schools. However, careful consideration should be given to the purpose for use, whether the processing is necessary and proportionate including the implications of using this technology for example, any operational requirements, the use of personal information and possible data breaches as well as the legal requirements associated with the management of it.

3.4 The data controller, must ensure that the processing of any biometric data, including any processing carried out by a third party on their behalf complies with the Data Protection Act 2018, UK GDPR and Protection of Freedoms Act 2012 (sections 26 to 28).

3.5 The Protection of Freedoms Act 2012 imposes a requirement on schools and colleges to obtain consent from parent of children under 18 years of age before processing the child's biometric information.

4. 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

5. The Legal Requirements under UK GDPR

5.1 '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.

5.2 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 by each individual Trust school.

6. Consent

6.1 Who can give consent

6.1.1 In order to comply with the requirements of the Protection of Freedoms Act 2012, school and colleges 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.

6.1.2 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 a school or college would notify and seek consent from to process personal biometric data. Any one parent could give or withhold consent.

6.1.3. 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, a school or college would not be required to notify or seek consent from birth parents.

6.2 Pupils' / students' right to refuse.

6.2.1 If a pupil/student under 18 objects or refuses to participate (or to continue to participate) in activities that involve the processing of their biometric data, the school or college must ensure that the pupil's/student's biometric data is not taken/used as part of a biometric recognition system. A pupil's/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.

6.3 Parents right to refuse.

6.3.1 If a parent objects to the processing, then the School will not be permitted to use that child's biometric data and alternatives will be provided.

6.4 Length of consent / Security of consent

6.4.1 The Trust would expect schools to carry out the following when considering security of biometric data:

- store biometric data securely to prevent any unauthorised or unlawful use
- not keep biometric data for longer than it is needed meaning that a Trust school should destroy a pupil's/student's biometric data if, for whatever reason, they no longer use the system including when leaving the school, where a parent withdraws consent or the pupil/student either objects or withdraws consent
- ensure that biometric data is used only for the purposes for which they are obtained and that such data are not unlawfully disclosed to third parties

6.4.2 Pupils/student and parents can also object at a later stage to the use of their child's/their biometric data. Should a parent/child wish to withdraw their consent, they can do so by writing to the School directly requesting that the School no longer use their child's biometric data

7. Alternative to Biometric

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

8. Biometric data and Processing

Processing' of biometric data 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:

- recording pupil/students' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner
- storing pupil/students' biometric information on a database system
- 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 pupil/students'