BIOMETRIC POLICY

Approved by the STAR MAT Trust Board	26 November 2020
Review Date	November 2023

Introduction

This Policy fulfils the STAR Multi-Academy Trust's obligation to have an appropriate policy document in place where the processing of Special Category Biometric data is in place.

The Biometric Policy governs the Trust's collection and processing of biometric data. The nature of this processing, including what information is processed and for what purpose, is outlined in the school's privacy notices.

The Trust will comply with the additional requirements of sections 26 to 28 of the Protections of Freedoms Act 2012, this includes provisions which relate to the use of biometric data in schools and colleges who use an automated biometric recognition system. These provisions are in addition to the requirements of GDPR.

This policy complements the school's existing records of processing required under Article 30 of the General Data Protection Regulation (GDPR) 2018, which is fulfilled through the School's Information Asset Register. It should also be read in conjunction with the other policies and privacy notices in the School's Information Governance policy and privacy notice framework.

Scope

All policies in the school's Information Governance policy framework apply to all Trust employees, any authorised agents working on behalf of the Trust, including temporary or agency employees, and third party contractors. Individuals who are found to knowingly or recklessly infringe these policies may face disciplinary action.

The policies apply to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper,
- Information or data stored electronically, including scanned images,
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer,
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card,
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops,
- Published web content, for example intranet and internet,
- Photographs and other digital images.

Definition of "Biometric Data"

Biometric data is defined as personal data relating to the physical, physiological or behavioural characteristic of an individual which allows the identification of that individual.

This can include their fingerprints, facial shape, retina and iris patterns, and hand measurements.

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. For example, where a fingerprint is used to identify an individual and allow them access to an account.

Biometric Data is defined in the GDPR 2018 and the Data Protection Act 2018 as a special category of personal data, and it therefore requires additional measures to be put in place in order to process it, as detailed below.

Definition of "Processing"

'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'/student's biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner;

b) Storing pupils'/student's biometric information on a database system; or

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/students.

Any processing of Biometric data will only be carried out where there is a lawful purpose for the processing, as defined under Article 6 and Article 9 (Schedule 1) of the GDPR 2018. The purposes will be outlined in the Trust's privacy notices which will be made available to the relevant individuals.

What Counts as Valid Consent?

The Data Protection Act 2018 states that an individual can consent to the use of their own personal data when they are considered to have the adequate capacity to fully understand what they are consenting to. Most individuals are considered to reach this capacity over the age of 12, however where the school considers the individual to not have adequate capacity to consent themselves, the consent of one or more of their parents/carers will be sought.

The school will ensure that the member of staff, or the pupil/student and both of their parents/carers (if possible) will be informed of the school's intention to process the individual's biometric data. This will be carried out through readily available privacy notices and communications, prior to or at the point of obtaining consent, and will include:

- The type of biometric data
- What it will be used for
- The parent's and pupil's/student's rights to withdraw or refuse consent
- What the alternative arrangement will be if consent is refused or withdrawn

Under no circumstances will the school collect or process the biometric data of an individual without their explicit consent or the consent of at least one authorised parent/carer, this will be obtained prior to obtaining any biometric data. If one parent objects in writing, then the school will not be permitted to take or use that child's biometric data.

All consent must be freely-given, specific, informed and unambiguous, and will be obtained through a clear affirmative action. The school will collect consent through consent forms for new starters and update forms.

Where the school collects additional Biometric data, or begins to process the biometric data for a new purpose, new consent must be gained to ensure that the individual or their parent/carer is fully informed. This consent must also meet all of the standards outlined in this section.

The Protection of Freedoms Act 2012 only covers processing on behalf of the Trust. If a pupil is using biometric software for their own personal purposes (e.g. facial recognition technology) this is classed as private use not processing by the Trust, even if the software is accessed using school or college equipment.

Length of Consent and Withdrawing Consent

The consent will be valid until it is withdrawn or until the Biometric data reaches the school's retention period, as outlined in the school's retention schedule and Information Asset Register/ when the student leaves the school, at which point the Biometric data and record of consent will be securely destroyed.

Consent can be withdrawn at any time by the parent/carer or the individual, by writing to the school requesting that the school no longer use their child's biometric data. If a student under the age of 18 objects to the processing of their Biometric data, this will override the consent of the parents/carers and processing will not continue under any circumstances.

Alternative to Biometric Data

The school will ensure that where consent is refused or withdrawn, there is an alternative solution which does not require the obtaining or processing of Biometric data. This will ensure that the consent is freely given and that no pressure is placed on the individual or their parent/carer to consent in order to take part in the school's processes.

Data Protection Impact Assessment

Where a new system involving Biometric data, or a new form of processing for Biometric data is introduced, the school will ensure that they have completed a Data Protection Impact Assessment (DPIA) to address any risks associated with the project prior to the implementation of the project. This will be sent to the Trust's Data Protection Officer for final approval.