THE 1590 TRUST PROTECTION OF BIOMETRIC INFORMATION POLICY

Date: *September 2022*

Policy Review Cycle: *Every 3 Years*

Review Assigned to: *Trust Board*

**Policy in practice for ratification at Trust Meeting on 14.12.22*

Statement of intent

The 1590 Trust is committed to protecting the personal data of all its staff and students which includes any biometric data collected and processed.

The 1590 Trust collects and processes biometric data in accordance with relevant legislation and guidance to ensure the data and the rights of individuals are protected. This policy outlines the procedure the Trust follows when collecting and processing biometric data and operates in conjunction with the Trust GDPR Policy.

Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- The Data Protection Act 2018
- The UK General Data Protection Regulations (GDPR)
- The Protection of Freedoms Act 2012
- The Department for Education (DfE) Guidance on the protection of biometric data of children in schools and colleges.

Definitions

Biometric data: Personal information about an individual's physical, psychological or behavioural characteristics that can be used to identify that person, including their fingerprints, facial images and voice recognition.

Automated biometric recognition system: A system 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.

Processing biometric data: Processing biometric data includes obtaining, recording or holding the data or carrying out any operation 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 students' biometric data, e.g. taking measurements from a fingerprint via a fingerprint scanner.
- Storing students' biometric information on a database.
- Using students' biometric data as part of an electronic process, e.g. by comparing it with biometric information stored on a database to identify or recognise students.

Special category data: Personal data which the GDPR says is more sensitive, and so needs more protection. Where biometric data is used for identification purposes, it is considered special category data.

Roles and responsibilities

1. The 1590 Trust Board is responsible for reviewing this policy every three years.

2. The Chief Executive and Trust School Headteachers/Head of School are responsible for ensuring the provisions of this policy are implemented consistently.

3. The Data Protection Officer (DPO) is responsible for:

    - Monitoring the Trust's compliance with data protection legislation in relation to the use of biometric data.
    - Advising on when it is necessary to undertake a data protection impact assessment (DPIA) in relation to the Trust's biometric system(s).
    - Being the first point of contact for the Information Commissioner's Office (ICO) and for individuals whose data is processed by the Trust and connected third parties.

Data protection principles

The Trust processes all personal data, including biometric data, in accordance with the key principles set out in the GDPR.

The 1590 Trust may use biometric data in a number of ways, including but not limited to:-

- Meal payments & topups
- Library / loans
- Tablet IT access (e.g. iPad Touch ID).

The Trust ensures biometric data is:

- Processed lawfully, fairly and in a transparent manner.
- Only used for the reason it was collected and not for additional or unrelated purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date.
- Kept for as long as is necessary for the purposes for which the personal data are processed, after which it will be securely destroyed or deleted.
- Processed in a manner that ensures appropriate security of the information.

Data protection impact assessments (DPIAs)

Prior to processing biometric data or implementing a system that involves processing biometric data, a DPIA will be carried out. The Data Protection Officer (DPO) will oversee and monitor the process of carrying out the DPIA which should:

- Describe the nature, scope, context and purposes of the processing.
- Assess necessity, proportionality and compliance measures.
- Identify and assess risks to individuals.
- Identify any additional measures to mitigate those risks.

When assessing levels of risk, the likelihood and the severity of any impact on individuals will be considered.

If a high risk is identified that cannot be mitigated, the DPO will consult the ICO before the processing of the biometric data begins and seek their advice.

Notification and consent

Where the Trust uses students' biometric data as part of an automated biometric recognition system (e.g. using students' fingerprints to receive school dinners instead of paying with cash), the Trust will comply with the Protection of Freedoms Act 2012.

Prior to processing a student's biometric data, where possible the Trust will notify the relevant parents/guardians of their intention to process the biometric information and request their consent to do so. Written consent will be sought from at least one parent of the student before the Trust collects or uses a student's biometric data. A student's objection or refusal will override any parental consent to the processing. A student does not have to object in writing but a parent's objection must be written.

When obtaining consent, the name and contact details of the student's parents will be taken from the Trust School's admission register.

Where the name of only one parent is included on the admissions register, the Trust School Headteacher/Head of School will consider whether any reasonable steps can or should be taken to ascertain the details of the other parent.

The Trust will not need to notify a particular parent or seek their consent if the Trust is satisfied that:

- The parent cannot be found, for example, his or her whereabouts or identity is not known .
- The parent lacks the mental capacity to object or to consent.
- The welfare of the student requires that a particular parent is not contacted.
- Where it is otherwise not reasonably practicable for a particular parent to be notified or for his or her consent to be obtained.

Where neither parent of a student can be notified for any of these reasons, consent will be sought from the following individuals or agencies as appropriate:

- If a student is being 'looked after' by the Local Authority (LA) or is accommodated or maintained by a voluntary organisation, the LA or voluntary organisation will be notified and their written consent obtained.
- If the above does not apply, then notification will be sent to all those caring for the student and written consent will be obtained from at least one carer before the student's biometric data is processed.

Notification sent to parents and other appropriate individuals or agencies will include information regarding the following:

1. Details about the type of biometric information to be taken.
2. How the data will be used.
3. The parent's and the student's right to refuse or withdraw their consent.
4. The Trust's duty to provide reasonable alternative arrangements for those students whose information cannot be processed.

The Trust will not process the biometric data of a student under the age of 18 in the following circumstances:

- The student objects or refuses to participate in the processing of their biometric data.
- No parent or carer has consented in writing to the processing.
- A parent has objected in writing to such processing, even if the other parent has given written consent.

Parents/guardians and students can object to participation in the Trust's biometric system(s) or withdraw their consent at any time. Where this happens, any biometric data relating to the student that has already been captured will be deleted and the Trust will seek to make alternative arrangements.

Where staff members or other adults use the Trust's biometric system(s), consent will be obtained from them before they use the system.

Staff and other adults can object to taking part in the Trust's biometric system(s) and can withdraw their consent at any time. Where this happens, any biometric data relating to the individual that has already been captured will be deleted.

Alternative arrangements will be provided to any individual that does not consent to take part in the Trust's biometric system(s), in line with this policy.

Alternative arrangements

Where an individual objects to taking part in the Trust's biometric system(s) the Trust will seek to make reasonable alternative arrangements to allow the individual to access the relevant service, e.g. where a biometric system uses students' fingerprints to pay for school meals, the student will be able to use cash for the transaction instead.

The Trust should work to ensure that alternative arrangements will not put the individual at any disadvantage, create difficulty in accessing the relevant service or result in any additional burden being placed on the individual and/or their parents/guardians where relevant.

Data retention

Biometric data will be managed and retained in line with data retention guidelines. If an individual (or a student's parent, where relevant) withdraws their consent for their/their child's biometric data to be processed, it will be deleted from the Trust's system.

Breaches

There are appropriate and robust security measures in place to protect the biometric data held by the Trust. Any breaches to the Trust's biometric system(s)/data will be dealt with in accordance with GDPR requirements and in line with the Trust's GDPR Policy.