Name of Policy	**PROTECTION OF BIOMETRIC INFORMATION POLICY**
Policy Number	**NS27**
The Three Rivers	
Named Person(s)	**Alison Hoyle**
Review Committee	**Full Board**
Last review date	Autumn 2019
Next review date	Autumn 2022

Key Changes	Registration Procedures
Sources	School Bus, Muckle LLp
Statutory/Non-Statutory	

Introduction

This policy is being introduced to comply with the Protection of Freedoms Act 2012, which comes into effect from September 2015.

The Three Rivers Learning Trust is committed to protecting the personal data of all its students and staff, this includes any biometric data we collect and process. We collect and process biometric data in accordance with relevant legislation and guidance to ensure the data and the rights of individuals are protected. This policy outlines the procedures we follow when collecting and processing biometric data.

Legal Framework

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

- Protection of Freedoms Act 2012
- Data Protection Act 2018
- General Data Protection Regulation (GDPR)
- DfE 2018 'protection of information of children in schools and colleges

This policy operates in conjunction with the following Trust policies:

- Data Protection Policy
- Records Management Policy
- Data and E-security Breach Prevent and Management Plan

Definitions

- **Biometric Data:** Personal information about an individual's physical or behavioural characteristics that can be used to identify that person, including their fingerprints, facial shape, retina and iris patterns and hand measurements
- **Automated biometric recognition system:** A system which measures an individual's physical or behavioural characteristics by using equipment that operates 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 disclosing it, deleting it, organising or altering it. An automated biometric recognition system processes data when:
    - Recording students' biometric data, eg 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, eg. 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

- The Board of Trustees is responsible for reviewing this policy every three years
- The Headteacher is responsible for ensuring the provisions in the policy are implemented consistently
- The data protection officer is responsible for monitoring the schools compliance in relation to the use of biometric data. Advising when it is necessary to undertake a data protection impact assessment in relation to the schools' biometric systems. Being the first point of contact for individuals whose data is processed by the school and connected third parties

Data Protection Principles

- The school processes all personal data,including biometric data, in accordance with the key principles set out in the GDPR
- The school ensures biometric data is:
    - Processed lawfully, fairly and in a transparent manner
    - Only collected for specific ,explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
    - Adequate,relevant and limited to what is necessary in relation to the purposes to which they are processed
    - Accurate and, where necessary, kept up-to-date, and that reasonable steps are taken to ensure inaccurate information is rectified or erased
    - Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
    - Processed in a manner that ensures appropriate security of the information, including protection against unauthorised or unlawful processing and against accidental loss,destruction or damage, using appropriate technical or organisational measures

Data protection impact assessments(DPIAs)

- Prior to processing biometric data a DPIA will be carried out
- The DPO will oversee and monitor this process
- The DPIA will
    - Describe the nature, scope, context and purposes of the processing
    - Assess necessity and compliance measures
    - Identify and assess risks to individuals
    - Identify and additional measures to mitigate those tasks when assessing levels of risk, the likelihood and severity of any impact on individuals will be considered
- If a high risk is identified that cannot be mitigated, the DPIO will consult the ICO before the processing of the data begins
- The ICO will provide the school with a written response (within eight weeks or 14 weeks in complex cases) advising whether the risks are acceptable, or whether the school needs to take further action
- The school will adhere to any advice from the ICO

Notification and Consent
Please note that the obligation to obtain consent for the processing of biometric information of children under the age of 18 is not imposed by the Data Protection Act 2018 ot the GDPR. Instead the consent requirements for biometric information is imposed by section 26 0f the Protection of Freedoms Act 2012.

Where the school uses students' biometric data as part of an automated biometric recognition system (eg using students' fingerprints to receive school meals instead of paying with cash), the school will comply with the requirements of the Protection of Freedoms Act 2012. Prior to any biometric recognition system being put in place or processing a students biometric data, the school will send the students parents/carers a Parental Notification and Consent Form for the use of Biometric Data. Written consent will be sought from at least one parent before the school collects or uses a students biometric data. The name and contact details will be taken from the schools admission register. The school does not need to notify a parent or seek their consent if it is satisfied that:

- The parent cannot be found
- The parent lacks the mental capacity to object or consent
- The welfare of the student requires that a particular parent is not contacted, eg where a student has been separated from and abusive parent who must not be informed of the students whereabouts
- It is not reasonably practicable for a particular parent to be notified or for their consent to be obtained

Where neither parent of a pupil can be notified for any reason, consent will be sought from the following:

- If a student is being 'looked after' by the 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 data can be processed

Notification sent to parents/carers and appropriate individuals or agencies will include the following information:

- Details about the type of biometric information to be taken
- How the data will be used
- The parents and the students right to refuse or withdraw consent
- The school's duty to provide reasonable alternative arrangements for those students whose information cannot be processed

The school 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 process
- No parents or carer has consented in writing
- A parent has objected in writing to the process, even if another parent has given written consent

Parents and students can object or withdraw their consent at any time. When this happens any biometric data relating to the student will be deleted. If a student objects or refuses to participate in the school will ensure that the biometric data is not taken or used as part of a biometric recognition system, irrespective of any consent given by the students parents.
Students will be informed that they can object or refuse their data to be collected via the introduction letter.

Where staff members or other adults use the biometric system consent will be obtained from them before they use the system.

Alternative Arrangements

- Parents, students and staff members have the right to not take part in the biometric system
- Where an individual objects reasonable alternatives will be provided that allows them to access the service eg they will be given a code to use
- Alternative arrangements will not put the individual at any disadvantage to access the service

Data Retention

- Biometric data will be managed in lines with the schools data protection policy

Breaches

- There are appropriate and robust security measures in place to protect the data held by the school

Monitoring and Review

- The Learning Trust Board of Directors will review this policy on a three yearly basis
- The next scheduled review date for this policy will be Autumn 2022
- Any changes made to this policy will be communicated to all staff, parents and students