ENDEAVOUR
LEARNING TRUST

PROTECTION OF BIOMETRIC INFORMATION POLICY

Endeavour Learning Trust

March 2021

1. INTRODUCTION

Endeavour Learning Trust (ELT) 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 ELT follow when collecting and processing biometric data.

This policy operates in conjunction with the ELT's GDPR Data Collection Policy.

Throughout this document the term Headteacher is used, but may be, for some schools, replaced with the term Executive Headteacher or their designated representative (usually a Head of School).

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
- UK General Data Protection Regulation (GDPR)
- DfE (2018) 'Protection of biometric information of children in schools and colleges'

2. 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 '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 disclosing it, deleting it, organising it or altering it. An automated biometric recognition system processes data when:

- Recording student biometric data, e.g. taking measurements from a fingerprint via a fingerprint scanner.
- Storing student biometric information on a database.
- Using student 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.

3. CASHLESS CATERING

ELT uses student information as part of the automated recognition system for the purposes of using cashless catering systems. ELT uses cashless catering facilities provided by Vericool and Biostore, companies which specialise in educational cashless catering and manage the biometrics and the payments for meals. The Tucasi and Schoolcomms online payments systems integrate with these systems.

In order to use the cashless catering system students simply place their fingertip on a scanner to make a payment for their food. The light on the biometric reader is used solely to illuminate the fingertip of the student or staff member and the scanning device then effectively takes a capture. Most of the data is discarded and only a limited number (approx. 120) of random points on the fingerprint are retained, not the whole fingerprint. These are not stored as images but are converted using a mathematical process to convert the image data to what is essentially a string of random numbers. The system does not record fingertips / fingerprints and an image of the student's fingerprint is not stored.

The information collected will be used solely for school purposes and held on the school system only. This technology is very secure and is commonly used within other schools across the UK.

4. ROLES AND RESPONSIBILITIES

The Headteacher is responsible for ensuring the provisions in this policy are implemented consistently.

The Data Protection Officer (DPO) is responsible for:

- Monitoring the school'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 systems.
- Being the first point of contact for the ICO and for individuals whose data is processed by the school and connected third parties.

5. DATA PROTECTION PRINCIPLES

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

ELT ensures biometric data is:

- Processed lawfully, fairly and in a transparent manner.
- Only collected for specified, 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 for 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.

As the data controller, the school is responsible for being able to demonstrate its compliance with the provisions outlined above.

6. 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 or the GDPR. Instead, the consent requirements for biometric information is imposed by section 26 of the Protection of Freedoms Act 2012.

Where ELT uses student's biometric data as part of an automated biometric recognition ELT will comply with the requirements of the Protection of Freedoms Act 2012. The Act requires ELT to notify each parent of a child (where known) and obtain the written consent of at least one parent before being able to use a child's biometric information for an automated system.

Written consent will be sought from at least one parent of the student before ELT collects or uses a student's biometric data. The 'Parental Consent for the Use of Biometric Information in School' form is completed and retained.

As stated above, in order to be able to use a student's biometric information, the written consent of at least one parent is required. However, consent given by one parent will be overridden if the other parent objects in writing to the use of their child's biometric information. Similarly, if the student objects to the use of their biometric information, then ELT cannot collect or use his/her biometric information for inclusion on the automated recognition system.

Parents and students can also object to the proposed processing of the biometric information at a later stage or withdraw any consent previously given. This means that, if consent is given but parents or students change their mind, they can withdraw this consent. Any consent, withdrawal of consent or objection from a parent must be in writing. Where this happens, any biometric data relating to the student that has already been captured will be deleted.

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

- 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 student's biometric data can be processed.

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

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

ELT will not process the biometric data of a student in the following circumstances:

- The student (verbally or non-verbally) 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 another parent has given written consent

If staff members or other adults wish to make use of ELT's biometric systems, their consent is implicit if they register to use the system.

Staff and other adults can withdraw from using ELT's biometrics systems at any time. Where this happens, any biometric data relating to the individual that has already been captured will be deleted.

Alternative payment arrangements will be provided to any individual that does not consent to take part in ELT's biometric system, this may include taking manual payments at the point of sale. These arrangements will be agreed with the Operations Managers.

Once a student or adult ceases to use the biometric recognition system, their biometric information is securely deleted from the cashless catering systems.

8. ALTERNATIVE ARRANGEMENTS

Parents, students, staff members and other relevant adults have the right to not take part in ELT's biometric systems.

Where an individual objects to taking part in ELT's biometric systems, reasonable alternative arrangements will be provided that allow the individual to access the relevant service, e.g. where a biometric system uses student's fingertips to pay for school meals, the student will be able to use an alternative method for the transaction.

Alternative arrangements will not put the individual at any disadvantage or create difficulty in accessing the relevant service, or result in any additional burden being placed on the individual and the student's parents.

6. DATA PROTECTION IMPACT ASSESSMENTS (DPIAs)

Prior to implementing a new system that involves processing biometric data, a DPIA will be carried out.

The DPO will oversee and monitor the process of carrying out the DPIA.

The DPIA will:

- 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.

9. POLICY REVIEW

This policy is reviewed annually by the Trust executive and agreed by the Trust Board.

Signed by:			
Mrs L Gwinnett	Trust Leader/CEO	Date	March 2021
Mrs H Dicker	Chair of Trustees		