UNIVERSITY OF LINCOLN

THE LINCOLNSHIRE EDUCATIONAL TRUST LTD

University Academy Holbeach

Executive Principal: Steven Baragwanath
Principal: Sheila Paige

Protection of Biometric Information Policy

Date:	February 2022
Adopted by the Governing Body	
Review Date:	February 2023

1. Policy Statement

The Lincolnshire Educational Trust Limited is committed to protecting the personal data of all its pupils 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 the trust follows when collecting and processing biometric data.

2. Biometric Information and How It Should Be Used

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

This policy operates in conjunction with the following Trust/Academy policies:

- Data Protection Policy

Definitions

Biometric data is:

- Personal information about an individual's physical or behavioural characteristics that can be used to identify that person; this can include their fingerprints, facial shape, retina and iris patterns, and hand measurements.
- Considered by the Information Commissioner to be personal data as defined by the Data Protection Act 2018; this means that it must be obtained, used and stored in accordance with that Act.

An automated biometric recognition system is:

- 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.

Processing biometric data is:

- "Processing" of biometric information including 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 pupils/staff biometric data e.g. taking measurements from a fingerprint via a fingerprint scanner.
    - Storing pupils/staff biometric information on a database.
    - Using pupils/staff biometric data as part of an electronic process e.g. by comparing it with biometric information stored on a database to identify or recognise pupils.

Roles and Responsibilities

The Governing Body is responsible for:

- Reviewing this policy on an annual basis.

The Executive Principal/Principal is responsible for:

- Ensuring the provisions in this policy are implemented consistently.

The Data Protection Officer (DPO) is responsible for:

- Monitoring the Trust/Academy'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 the Trust/Academy's biometric system(s).
- Being the first point of contact for the ICO and for individuals whose data is processed by the Trust/Academy and connected third parties.

Data Protection Principles

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

The Trust/Academy 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 Trust is responsible for being able to demonstrate its compliance with the provisions outlined above.

Data Protection Impact Assessments (DPIA)

Prior to processing biometric data or implementing a 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.

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

The ICO will provide the Trust/Academy with a written response (within eight weeks or 14 weeks in complex cases) advising whether the risks are acceptable, or whether the Trust/Academy needs to take further action. In some cases, the ICO may advise the Trust/Academy to not carry out the processing.

The Trust/Academy will adhere to any advice from the ICO.

3. Providing Your Consent/Objecting

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

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

Written consent will be sought from at least on parent of the pupil before the Trust/Academy collects or uses a pupil's biometric data.

The name and contact details of the pupil's parents will be taken from the Academy's admission register.

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

The Trust/Academy does not need to notify a particular parent or seek their consent if it is satisfied that:

- The parent cannot be found e.g. their whereabouts or identity is not known.
- The parent lacks the mental capacity to object or consent.
- The welfare of the pupil requires that a particular parent is not contacted e.g. where a pupil has been separated from an abusive parent who must not be informed of the pupil's whereabouts.
- It is otherwise not reasonably practicable for a particular parent to be notified or for their consent to be obtained.

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

- If a pupil is being "looked after" by the local authority or is accommodated or maintained by a voluntary organisation, the local authority 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 pupil and written consent will be obtained from at least one carer before the pupil's biometric data can be processed.

Notification 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 pupil's right to refuse or withdraw their consent.
- The Trust/Academy's duty to provide reasonable alternative arrangements for those pupils whose information cannot be processed.

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

- The pupil (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.

Parents and pupils can object to participation in the Trust/Academy's biometric system(s) or withdraw their consent at any time. Where this happens, any biometric data relating to the pupil that has already been captured will be deleted.

If a pupil objects or refuses to participate, or to continue to participate, in activities that involve the processing of their biometric data, the Trust will ensure that the pupil's biometric data is not taken or used as part of a biometric recognition system, irrespective of any consent given by the pupil's parent(s).

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

Parents, pupils, staff members and other relevant adults have the right to not take part in the Trust/Academy's biometric system(s).

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

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 pupil's parents, where relevant).

Data Retention

Biometric data will be managed and retained in line with other Trust/Academy policies.

If an individual (or a pupil's parent, where relevant) withdraws their consent for their/their child's biometric data to be processed, it will be erased from the Trust's system.

Monitoring and Review

The Governing Body will review this policy on an annual basis.

The updated policy will be made available to all staff, parents and pupils on the Trust/Academy website.

Please note that, when your child leaves the Academy or ceases to use the biometric system, their biometric information will be securely erased in line with the Trust's policies.

4. Further Information and Guidance

This can be found via the following links:

Department for Education's "Protection of Biometric Information of Children in Schools – Advice for proprietors, governing bodies, head teachers, principals and school staff":

- https://www.gov.uk/government/publications/protection-of-biometric-information-of-children-in-schools

ICO guide to data protection:

- https://ico.org.uk/for-organisations/guide-to-data-protection/

ICO guidance on data protection for education establishments:

- https://ico.org.uk/for-organisations/in-your-sector/education/

British Standards Institute guide to biometrics:

- https://shop.bsigroup.com/en/Browse-by-Subject/Biometrics/?t=r