BIOMETRICS POLICY

This policy applies to all the academies in The Lionheart Educational Trust

November 2025 – November 2027

Contents

The Lionheart Educational Trust systems

For the avoidance of doubt, whilst this policy exists to for fill our legal requirements, The Lionheart Educational Trust does not have any automated biometric recognition systems.

1.0 Introduction:

1.1 Biometric data means personal data obtained from specific technical processing of an individual's physical, physiological or behavioural characteristics, such as fingerprints, facial geometry, iris or retina patterns, or hand measurements, which enable or confirm unique identification of that individual.

1.2 The Lionheart Educational Trust schools and colleges treat the data they collect, including biometric data, with appropriate care and comply with the data protection principles as set out in the Data Protection Act 2018.

1.3 Where the data is to be used as part of an automated biometric recognition system, the Trust also complies with the additional requirements in sections 26 to 28 of the Protection of Freedoms Act 2012.

1.4 The Trust Schools and colleges will ensure that each authorised adult of a child is notified of the school's intention to use the child's biometric data as part of an automated biometric recognition system.

1.5 The Trust will obtain written consent of at least one authorised adult before the data is taken from the child and used. This applies to all registered pupils in Trust schools and colleges. In no circumstances can a child's biometric data be processed without written consent.

1.6 Trust Schools and colleges will not process the biometric data of a pupil (under 18 years of age) where:

- The child (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data;
- No authorised adult has consented in writing to the processing; or
- An authorised adult has objected in writing to such processing, even if another authorised adult has given written consent.

1.7 Trust schools and colleges must provide reasonable alternative means of accessing services for those pupils who will not be using an automated biometric recognition system. 3

2.0 Automated biometric recognition system

2.1 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.

2.2 For the avoidance of doubt, whilst this policy exists to for fill our legal requirements, The Lionheart Educational Trust does not have any automated biometric recognition systems.

2.3 Before introducing any automated biometric recognition system, the Trust will complete a Data Protection Impact Assessment (DPIA) in accordance with UK GDPR and ICO guidance. The DPIA will assess risks to individuals' rights and freedoms and identify measures to mitigate those risks.

3.0 Processing biometric data

3.1 *'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:

- Recording pupils' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner;
- Storing pupils' biometric information on a database system; or
- 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.

4.0 Gaining consent for the processing of biometric data:

4.1 The Trust commits to ensuring authorised adult and children can make an informed choice about the processing of their biometric data. The Trust will ensure authorised adults receive full information about the processing of their child's biometric data including a description of the kind of system they plan to use, the nature of the data they process, the purpose of the processing and how the data will be obtained and used. Students will be provided with information in a manner that is appropriate to their age and understanding.

4.2 The Trust will notify each authorised adult of a child whose biometric information they wish to collect/use. If one authorised adult objects in writing, then the Trust will not to take or use that child's biometric data.

4.3 Should a child object to their processing of biometric data, the Trust does not require the student to object in writing. An older child may be more able to say that they object to the processing of their biometric data. A younger child may show reluctance to take part in the physical process of giving the data in other ways. In either case the Trust will not collect or process the data.

4.4 Schools are not required by law to consult authorised adults before installing an automated biometric recognition system. However, the Trust commits to notifying authorised adults and securing consent from at least one authorised adult before biometric data is obtained or used for the purposes of such a system or if a new different type of automated biometric recognition system is introduced.

5.0 Conditions where consent is not needed:

5.1 The Trust Schools and colleges will not need to notify a particular authorised adult or seek their consent if the school or college is satisfied that:
a. the authorised adult cannot be found, for example, his or her whereabouts or identity is not known;
b. the authorised adult lacks the mental capacity to object or to consent;
c. the welfare of the child requires that a particular authorised adult is not contacted, for example where a child has been separated from an abusive authorised adult who is not to be informed of the child's whereabouts; 4 or d. where it is otherwise not reasonably practicable for a particular authorised adult to be notified or for his or her consent to be obtained.

6.0 Objecting or withdrawing consent:

6.1 The Trust will ensure that pupils understand that they can object or refuse to allow their biometric data to be taken/used and that, if they do this, the Trust will provide them with an alternative method of accessing relevant services.

6.2 **Authorised adult**

The original written consent is valid until such time as it is withdrawn (in writing). Consent can also be overridden, at any time if another authorised adult objects to the processing (subject to the objection being in writing).

6.3 **Children**

A child can object to the processing of their biometric data or refuse to take part at any stage – i.e. before the processing takes place or at any point after his or her biometric data has been obtained and is being used as part of a biometric recognition system. If a pupil objects, the Trust will not start to process his or her biometric data or, if they are already doing this, must stop. The child does not have to object in writing.

7.0 Retention of biometric data

7.1 When the pupil leaves any of the Trust schools and colleges, their biometric data will be securely removed from the school's biometric recognition system in conjunction with the Trust Data Protection policy.

7.2 The Trust will implement appropriate technical and organisational measures to protect biometric data, including encryption, restricted access controls, and audit trails. These measures will be reviewed regularly

8.0 Use of photographs and CCTV:

8.1 Consent is not required for the use of photographs and CCTV in schools, unless the use of photographs and CCTV is for the purpose of an automated biometric recognition system. More information about CCTV is contained in the Trust Data Protection Policy and the Trust CCTV Policy.

9.0 Protection of Freedoms Act 2012

9.1 The provisions in the Protection of Freedoms Act 2012 only cover processing by or on behalf of a school or college. If a Trust school or college wishes to use such software for school work or any school business, then the Trust will notify authorised adults and obtain written consent. However, if a pupil is using this software for their own personal purposes then there is no obligation on the Trust to gain consent, even if the software is accessed using school or college equipment.