DDAT

Derby Diocesan Academy Trust

Biometric Information Policy

May 2026

Approved by Trust Board on: 10th July 2026

Review date: May 2027

LTC reviewed: September 2026

Contents

1. Biometric Information Definition 2
2. Automated Biometric Recognition Systems 2
3. Why Biometric Information Is Used 2
4. Biometrics at All Saints, Bakewell CE Infants,Darley Churchtown and St. Giles 2
5. Notification and Consultation 2
6. Biometric Data Classification 3
7. Data Protection Impact Assessments 3
8. Lawful Basis for Processing Biometrics Data 4
9. Consent Requirements 4
9.1 Staff 4
9.2 Pupils 4
9.3 Consent limitations 5
9.4 Withdrawal of Consent 5
9.5 Alternative arrangements 5
10. Roles and Responsibilities 5
11. Relevant Legislation 6

1. Biometric Information Definition

Biometric data is personal information about an individual's physical or behavioural characteristics that can be used to identify that person.

This includes, but is not limited to, their fingerprints, facial shape, retina and iris patterns, and hand measurements.

2. Automated Biometric Recognition Systems

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.

To be recognised, an individual must have been previously subject to "enrolment". This is the process where samples of biometric data, such as fingerprints, are captured from an individual and stored to allow comparison in the future.

Further information can be found at: https://www.ncsc.gov.uk/collection/biometrics

3. Why Biometric Information Is Used

1. Biometric systems can be faster than using passwords or manual processes.
2. Biometrics can be more convenient, as they cannot be lost, misplaced or damaged.
3. Biometrics provide additional security as they cannot be stolen or loaned to someone else.

4. Biometrics at All Saints CE Infants, All Saints CE Junior, Bakewell CE Infants, Darley Churchtown and St. Giles CE Primary School and Nursery

The schools within the partnership do not use biometric information.

5. Notification and Consultation

All Saints CE Infants, All Saints CE Junior, Bakewell CE Infants, Darley Churchtown and St. Giles CE Primary School and Nursery will ensure that each parent 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.

Notification must be in line with the requirements detailed in the DfE document "Protection of biometric information of children in schools and colleges".

6. Biometric Data Classification

Where biometric data is used for identification purposes, it is considered special category data as defined by the General Data Protection Regulations (UK GDPR) and Data Protection Act 2018 (DPA 2018).

Each school is registered with the ICO as a data controller and complies with data protection legislation and principles. The schools must only use biometric data collected lawfully and with appropriate care.

The Protection of Freedoms Act 2012 includes provisions which relate to the use of biometric data in schools, when it is used as part of an automated biometric recognition system.

These provisions are in addition to the requirements of the Data Protection Act 2018 and are laid out in sections 26 to 28 of the Protection of Freedoms Act 2012.

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

7. Data Protection Impact Assessments

'Processing' of biometric information includes obtaining, recording, storing, disclosing, analysing, using, deleting, organising or modifying it.

An automated biometric recognition system processes data when:

1. Biometric data is recorded, for example, capturing a fingerprint via a fingerprint scanner.
2. Storing biometric information on a database or as part of a purchased system.
3. Using the recorded biometric data as part of an electronic process, to identify or recognise individuals.

A Data Protection Impact Assessment (DPIA) must therefore be carried out before any biometric data system is purchased or implemented, assessing any risks to data subjects and the measures the school will take to minimise the risks. This is in line with UK GDPR legal requirements.

The DPIA must document amongst other things, the purpose of the processing, the lawful basis, and the period of time the biometric information will be retained by the processor.

The DPO will oversee and monitor the process of carrying out the DPIA, but the decision to purchase and implement a system should be taken by the LTC and or/Trust Board.

When assessing levels of risk, the likelihood and the severity of any impact on individuals must be considered prior to the processing of any biometric data.

8. Lawful Basis for Processing Biometrics Data

Biometric data is classified as Special Category data under the GDPR and DPA 2018. Therefore, a lawful basis for processing under Article 9 of the UK GDPR must be identified by the school in addition to a lawful basis under Article 6 of the UK GDPR.

The lawful basis for the purposes of processing biometrics data of children in an education setting, is Explicit Consent (Article 9(2)(a)).

This requirement for consent for processing children's biometric information is imposed by section 26 of the Protection of Freedoms Act 2012.

The written consent of at least one parent must be obtained before the data is taken from the child and used (i.e. 'processed'). This applies to all pupils in schools and colleges under the age of 18. In no circumstances will a child's biometric data be processed without written consent.

In addition, even if a parent consents, the child may object to the processing of their biometric data or refuse to cooperate with the biometric data collection or use. The child's objection/refusal takes precedent over the parents' consent.

Measures must be put in place to ensure children can still access all services, etc. that the biometric data processing is designed to allow access to, even if they do not have their biometric data processed.

Further information can be found in the ICO guidance on data protection for education establishments. In relation to Facial Recognition Technology, the ICO have published a case study which sets out useful guidance on the data protection implications of such processing.

9. Consent Requirements

9.1 Staff

Each school is are obliged to obtain consent for the processing of any biometric information, whether for adults and children.

Consent should be sought from staff members or other adult stakeholders prior to the processing of their biometric data.

9.2 Pupils

Written consent must be sought from at least one parent of any child or young person under the age of 18.

Consent given by one parent will be overridden if the other parent objects in writing to the use of their child's biometric information. Objections should be addressed to the Headteacher.

Parental consent can also be overridden by the child.

For looked after pupils, the LA must be notified and notification will also be sent to all those caring for the pupil. Written consent must be obtained from at least one carer before the pupil's biometric data can be processed.

9.3 Consent limitations

Where the school only holds contact information for only one parent, staff should consider whether any reasonable steps can or will be taken to ascertain the details of the other parent.

Each school does not need to notify a particular parent or seek their consent if it is satisfied that:

- The parent cannot be found, after reasonable steps have been taken
- The parent lacks the mental capacity to object or consent.
- Welfare or safeguarding concerns require that a particular parent is not contacted.
- It is not practicable for a particular parent to be contacted.

9.4 Withdrawal of Consent

Where consent is withdrawn by an individual, or the parent of a pupil under 18, biometric data relating to that individual must be erased from the system.

Staff and other adults can object to the collection of their biometric data and can withdraw their consent at any time. If consent is withdrawn any biometric data relating to the individual that has already been captured must be deleted.

9.5 Alternative arrangements

Alternative arrangements must be provided to any individual that does not consent to the processing of their biometric information.

Where an individual objects to taking part in the school's biometric data processing system(s), reasonable alternative arrangements must be provided that allow the individual to access the relevant service. Each school will continue to offer a range of services which do not require biometric identification (such as payments via Arbor).

The school must ensure alternative arrangements do not put an individual (or the parents of pupils) at any disadvantage, create access difficulties or result in additional burdens.

10. Roles and Responsibilities

1. School LTC's and DDAT Trustees are responsible for reviewing this policy annually.
   LTC members/Trustees should also refer to guidance published in relation to the protection of children's biometric information in schools.

2. The Headteacher is responsible for ensuring this policy is communicated to all relevant stakeholders and the provisions in this policy are implemented consistently.

3. The Data Protection Officer (DPO) is responsible for advising of any necessary data protection impact assessment (DPIA) in relation to biometric system(s).
   The DPO is also the first point of contact for the ICO.

11. Relevant Legislation

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 (UK GDPR)
- DfE (2022) 'Protection of biometric information of children in schools and colleges'

This policy operates in conjunction with the following trust policies:

- Data Protection Policy
- Information Security Policy
- Records Retention Policy