



# Protection of Biometric Information Policy

Document date: December 2025



*Together, pursuing life in all its fullness*

<b>Version</b>	<b>Date</b>	<b>Author</b>	<b>Changes</b>
V1.0	July 2020	Peter Blenkinsopp	Initial Issue
V1.1	July 2021	Louise Beale	Reviewed, no material changes
V1.2	May 2023	Louise Beale	Reviewed, no material changes
V1.3	December 2025	Deb Bacon	Reviewed, no material changes, links updated.

<b>Review frequency</b>	2 years
<b>Review date</b>	December 2027
<b>Ratified by</b>	Board
<b>Date of ratification</b>	10 <sup>th</sup> December 2025
<b>Lead/owner</b>	Head of Operations and Compliance
<b>Target audience</b>	Staff, Parents and Public
<b>Document reference</b>	POL-DP10

The electronic version is the definitive version of this document.

## **CONTENTS**

1. Policy Statement
2. Definitions
3. Key Points
4. Data Protection principles
5. Privacy Impact Assessment
6. Notification and Consent
7. Alternative Arrangements
8. Retention of Biometric Data
9. Review of Policy and Biometric Recognition System
10. Misuse of Biometric Recognition Systems
11. Complaints Relating to this Policy
12. Further Information and Guidance

## BIOMETRIC INFORMATION POLICY

We are part of The Diocese of Coventry Multi Academy Trust (the Trust), a data controller for the purposes of data protection laws. Throughout this document, references to 'we', 'our', 'us' or the academy refer to the academy as part of The Diocese of Coventry Multi Academy Trust.

The Trust 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 procedure all of our academies follow when collecting and processing biometric data.

### 1 Policy Statement

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

- 1.1.1 Data Protection Act 2018
- 1.1.2 General Data Protection Regulation (GDPR)
- 1.1.3 Protection of Freedoms Act 2012
- 1.1.4 DfE (2018) 'Protection of biometric information of children in Academies and colleges'

1.2 This policy operates in conjunction with the following Trust policies:

- 1.2.1 Data Protection Policy
- 1.2.2 Data Retention Schedule

### 2 Definitions

- 2.1 **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.
- 2.2 **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.
- 2.3 **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:
  - 2.3.1 Recording pupils' biometric data, e.g. taking measurements from a fingerprint via a fingerprint scanner.

- 2.3.2 Storing pupils' biometric information on a database.
- 2.3.3 Using pupils' 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.
- 2.4 **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 Key Points

- 3.1 The Information Commissioner's Office (ICO) considers all biometric information to be personal data as defined by the GDPR; this means that it must be obtained, used and stored in accordance with this legislation.
- 3.2 The Protection of Freedoms Act includes provisions which relate to the use of biometric data in Academies and colleges when used as part of an automated biometric recognition system. These provisions are in addition to the requirements of the GDPR (see the Protection of Freedoms Act 2012 below).
- 3.3 Academies that use students' biometric data must treat the data collected with appropriate care and must comply with the data protection principles as set out in the GDPR.
- 3.4 Where the data is to be used as part of an automated biometric recognition system, academies must also comply with the additional requirements in sections 26 to 28 of the Protection of Freedoms Act 2012.
- 3.5 Academies must ensure that the parent/carers of each child is informed of the intention to use the child's biometric data as part of an automated biometric recognition system.
- 3.6 The written consent of the parent/carers or the child, where the child is deemed to have the capacity to consent (see below), must be obtained before the data is taken from the child and used (i.e. 'processed'). In no circumstances can a child's biometric data be processed without written consent.
- 3.7 Academies must not process the biometric data of a student where:
  - 3.7.1 The child (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data;
  - 3.7.2 A parent or student has not consented in writing to the processing; or
  - 3.7.3 A parent or student has objected in writing to such processing, even if another parent has given written consent.
- 3.8 Academies must provide reasonable alternative means of accessing the services to those students who will not be using an automated biometric recognition system.

## **4 Data Protection Principles**

- 4.1 The academies process all personal data, including biometric data, in accordance with the key principles set out in the GDPR. The academies ensure biometric data is:
  - 4.1.1 Processed lawfully, fairly and in a transparent manner.
  - 4.1.2 Only collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes.
  - 4.1.3 Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
  - 4.1.4 Accurate and, where necessary, kept up-to-date, and that reasonable steps are taken to ensure inaccurate information is rectified or erased.
  - 4.1.5 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.
  - 4.1.6 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.
- 4.2 As part of the Trust, which is the data controller, the academy is responsible for being able to demonstrate its compliance with the provisions outlined in this policy.

## **5 Privacy Impact Assessment**

- 5.1 Prior to processing biometric data or implementing a system that involves processing biometric data, a Data Protection Impact Assessment (DPIA) will be carried out.
- 5.2 The Data protection Officer (DPO) will oversee and monitor the process of carrying out the DPIA.
- 5.3 The DPIA will:
  - 5.3.1 Describe the nature, scope, context and purposes of the processing.
  - 5.3.2 Assess necessity, proportionality and compliance measures.
  - 5.3.3 Identify and assess risks to individuals.
  - 5.3.4 Identify any additional measures to mitigate those risks.
- 5.4 When assessing levels of risk, the likelihood and the severity of any impact on individuals will be considered.
- 5.5 If a high risk is identified that cannot be mitigated, the DPO will consult the ICO before the processing of the biometric data begins.

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

## **6 Notification and Consent**

- 6.1 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.
- 6.2 Where the Trust/academies use pupils and staff biometric data as part of an automated biometric recognition system (e.g. using pupils' fingerprints to receive academy dinners instead of paying with cash), the Trust/academy will comply with the requirements of the Protection of Freedoms Act 2012.
- 6.3 Written consent will be sought from at least one parent of the pupil before the academy collects or uses a pupil's biometric data.
- 6.4 The name and contact details of the pupil's parents will be taken from the school's information management system.
- 6.5 Where the name of only one parent is included on the admissions register, the Headteacher of the academy will consider whether any reasonable steps can or should be taken to ascertain the details of the other parent.
- 6.6 The academy does not need to notify a particular parent or seek their consent if it is satisfied that:
- 6.6.1 The parent cannot be found, e.g. their whereabouts or identity is not known.
  - 6.6.2 The parent lacks the mental capacity to object or consent.
  - 6.6.3 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.
  - 6.6.4 It is otherwise not reasonably practicable for a particular parent to be notified or for their consent to be obtained.
- 6.7 Where neither parent of a pupil can be notified for any of the reasons set out in 6.6, consent will be sought from the following individuals or agencies as appropriate:
- 6.7.1 If a pupil is being 'looked after' by the Local Authority (LA) or is accommodated or maintained by a voluntary organisation, the LA or voluntary organisation will be notified, and their written consent obtained.
  - 6.7.2 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.

- 6.8 Notification sent to parents and other appropriate individuals or agencies will include information regarding the following:
- 6.8.1 Details about the type of biometric information to be taken - How the data will be used.
  - 6.8.2 The parent's and the pupil's right to refuse or withdraw their consent.
  - 6.8.3 The Trust/academies duty to provide reasonable alternative arrangements for those pupils whose information cannot be processed.
  - 6.8.4 The Trust/academy will not process the biometric data of a pupil under the age of 18 in the following circumstances:
    - 6.8.4.1 The pupil (verbally or non-verbally) objects or refuses to participate in the processing of their biometric data.
    - 6.8.4.2 No parent or carer has consented in writing to the processing.
    - 6.8.4.3 A parent has objected in writing to such processing, even if another parent has given written consent.
  - 6.8.5 Parents and pupils can object to participation in the academies 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.
  - 6.8.6 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).
  - 6.8.7 Where staff members or other adults use the Trust's biometric system(s), consent will be obtained from them before they use the system.
  - 6.8.8 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 section 7 of this policy.

## **7 Alternative Arrangements**

- 7.1 Parents/carers, pupils, staff members and other relevant adults have the right to not take part in the academies biometric system(s).
- 7.2 Where an individual objects to taking part in the academies biometric system(s), reasonable alternative arrangements will be provided that allow the individual to access the relevant service. For example, where a biometric system uses pupils' fingerprints to pay for meals, the academy, or its third party, will provide the parent/carers with a PIN number.



- 7.3 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/carers, where relevant).

## **8 Retention of Biometric Data**

- 8.1 Biometric data will be managed and retained in line with the Trust's Data Retention Schedule.
- 8.2 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 academies system.

## **9 Review of Policy and Biometric Recognition System**

- 9.1 This policy will be reviewed every two years.
- 9.2 The biometric recognition system and the privacy impact assessment relating to it will be reviewed every two years.

## **10 Misuse of Biometric Recognition Systems**

- 10.1 The misuse of a biometric recognition system could constitute a criminal offence.
- 10.2 Any member of staff who breaches this policy may be subject to disciplinary action.

## **11 Complaints Relating to this Policy**

- 11.1 Any complaints relating to this policy or to the biometric recognition system operated by the Trust/academy should be made in accordance with the Trust's Complaints Policy.

## **12 Further Information and Guidance**

Further information on this topic may be obtained through the following links:

Department for Education "Protection of children's biometric information in schools"

[Protection of children's biometric information in schools - GOV.UK](#)

ICO Guidance on data protection for Schools:

[Schools, universities and colleges | ICO](#)