Bishop Chadwick
Catholic Education Trust

Biometrics Policy

Updated December 2024

Initially agreed by Directors: July 2022
Review Date: December 2026

Table of Contents

1. Purpose

This policy aims to ensure that the Bishop Chadwick Catholic Education Trust and associated schools collect and process pupil biometric data with appropriate care and in full compliance with the Data Protection Act 2018 and UK General Data Protection Regulation.

The Headteacher is responsible for the processing of biometric data including collecting, using, securing, and compliance with this policy.

This policy will be reviewed bi-annually by the Board of Directors to assess whether the use of the biometric data remains justified, necessary, and proportionate. Changes to legislation, national guidance or codes of practice may also trigger interim reviews.

2. Scope

This policy applies to all staff, pupils, third parties and visitors who may visit the school and includes the use of all surveillance technology used by the school.

Linked Documentation

This policy should be read in conjunction with the following documents:

- Data Protection Policy
- Acceptable Use of IT Systems Policy
- Information and Cyber Security Policy
- Data Retention Policy
- Keeping Children Safe in Education

3. Risk Appetite

The Trust has no appetite for regulatory breaches or breaches of this policy and related procedures.

4. Compliance

Where personal data is used as part of an automated biometric recognition system, the school must comply with the DPA 2018, UK GDPR and Protection of Freedoms Act 2012.

The school will notify each parent and the child of its intention to use the child's biometric data. Written consent of at least one parent must be obtained before any data is collected and used. In no circumstances can the child's biometric data be processed without prior written consent.

If a pupil of any age objects or refuses to participate or continue to participate in activities that involve their biometric data, the school must ensure that they do not collect or use it. A pupil's refusal overrides any parental consent.

The school must provide a reasonable alternative means of accessing services for those pupils who will not use the biometric recognition system.

The school takes steps to ensure that pupils and parents understand that they can object to the use of their biometric data being collected or used and an alternative method of accessing the relevant services is available to them. Alternative methods may include a key card or pin number.

The school ensures that no pupils who require alternative arrangements will suffer any disadvantage as a result of not participating.

5. Use of biometric data

Biometric data means 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.

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 to recognise or identify the individual.

Prior to using biometric data or implementing a system that involves processing biometric data, a Data Protection Impact Assessment (DPIA) must be completed and continuously reviewed. Examples of such instances include significant changes to an existing biometric system, such as switching to a new supplier or using a different type of biometric data compared to what was previously used.

Processing biometric data includes obtaining, recording, 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 students' biometric data. For example, taking measurements via a fingerprint scanner
- Storing students' biometric information on a database
- Using students' biometric data as part of an electronic process, for example 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 and the highest standards of technical and organizational standards must be applied.

6. Data retention

Biometric data will be managed and retained in line with the Trust's document retention schedule.

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