PROTECTION OF CHILDREN'S BIOMETRIC INFORMATION POLICY

for adoption by all CDAT schools

This policy is informed by the Christian values which are the basis for all of CDAT's work and any actions taken under this policy will reflect this.

'*Blessed are those who act justly, who always do what is right*'

Psalm 106:3

Approved by	Date	Review Schedule	Date of next review
Trust Board	September 2024	Annually	September 2025

1. Introduction

This policy may not be relevant to all schools within the trust, as the number of primary schools that use biometric data is still relatively small. However, this policy confirms CDAT's commitment to protecting information in line with best practice and allows for further innovation in this field within individual schools.

It would be strongly recommended that any CDAT school looking to introduce a system using biometric data should discuss plans with the CEO or DoO and the DPO, and may be asked to provide a briefing for the CDAT board to outline their thoughts and protective steps planned. Any school looking at introducing such a system would be expected to fully comply with the latest best guidance from DfE: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1092507/Biometrics_Guidance_July_2022.pdf

2. What is biometric data?

- Biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allows or confirms the unique identification of that natural person, such as facial imaging.
- The Information Commissioner considers all biometric information to be sensitive personal data as defined by the GDPR 2018; this means that it must be obtained, used and stored in accordance with that Regulation.
- The Protection of Freedoms Act 2012 includes provisions which relate to the use of biometric data in schools and colleges when used as part of an automated biometric recognition system. These provisions are in addition to the requirements of the GDPR 2018.

3. What is an automated biometric recognition system?

- 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. For example, some systems allow pupils to 'pay' for their school lunches in a cashless way by scanning their fingerprint.
- Biometric recognition systems can use many kinds of physical or behavioural characteristics such as those listed above.

4. What does processing data mean?

'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;
- 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

5. Introducing a Biometric System

Any CDAT schools introducing a Biometric System (e.g. for lunches, or to monitor library loans) will adhere closely to established best policy in this field, including:

- Communicating clearly with parents if/when a Biometric System is being considered, and any changes that are subsequently made; there is no statutory duty to consult with parents, but parents' views are important and so mechanisms need to be put in place to ensure they are adequately considered
- Providing parents with detailed information about any such system being introduced, so that they are able to make a fully informed decision as to whether or not to give consent for their child/children to use the system and to have their biometric data stored
- Making all reasonable efforts to ensure that consent given is genuine
- To ensure children without consent to have their biometric data stored are not unfairly disadvantaged and are still able to access all school facilities/activities

6. Protecting Data

The trust's approach to data protection is set out in the **Data Protection Policy**. Across the trust, we will ensure that personal information is dealt with properly and securely and in accordance with the relevant legislation. This applies to personal information, including biometric data, regardless of the way it is used, recorded and stored, and applies to personal information held in both paper and electronic files.