Aletheia Anglican Academies Trust

Protection of Biometric Information Policy

Review Body:	Board of Trustees
Leadership Group Responsibility:	Chief Operating Officer / Data Protection Officer
Policy Type:	Statutory
Adopted:	December 2020
Date of Next Review:	December 2022
Review Period:	2 Years

This procedure was adopted by the Board of Trustees of Aletheia Anglican Academies Trust, for implementation in all Trust academies on the date above and supersedes any previous Protection of Biometric Information Policy.

1. Introduction

1.1 The Trust is committed to protecting the personal data of all stakeholders, including any biometric data we collect and process.

1.2 This policy has due regard to relevant legislation, including the following:

- Data Protection Act 2018
- General Data Protection Regulation (GDPR)
- Protection of biometric information of children in schools and colleges (DfE, March 2018)
- The Protection of Freedoms Act 2012

2. What Is Biometric Data?

2.1 Biometric data means personal information about an individual's physical or behavioural characteristics that can be used to identify that person. This can include, but is not limited to, their fingerprints, facial shape, retina and iris patterns, recognition of speech / voice, and hand measurements.

2.2 The Information Commissioner considers all biometric information to be personal data as defined by the Data Protection Act 2018; this means that it must be obtained, used, and stored in accordance with that Act.

2.3 The Protection of Freedoms Act 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 Data Protection Act 2018.

2.4 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 securely stored in one or more system(s) to see if there is a match to recognise or identify the individual.

3. What Is Biometric Data Processing?

3.1 Processing of biometric information includes obtaining, recording or storage of 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.

3.2 An automated biometric recognition system processes data when:

- Recording students' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner
- Storing students' 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 to identify or recognise students

4. Data Protection Principles

4.1 The Trust processes all personal data, including biometric data, using the key principles set out in the GDPR.

4.2 The Trust will be responsible for compliance, ensuring biometric data is:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes and is not considered to be incompatible and / or disproportionate regarding its intended purposes
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- 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
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures

5. Consent

5.1 Where the Trust uses biometric data as part of automated biometric systems, the Trust will comply with the requirements stated in the Protection of Freedoms Act 2012.

5.2 Separate written consent will be sought from at least one parent or carer of the student before the Trust collects or uses a student's biometric data.

5.3 The Trust will not process biometric data of a student (under the age of 18) where:

- The student refuses to participate in the processing of biometric data
- No parent or carer has provided consent in writing for the processing of biometric data
- A parent or carer has refused to the processing of biometric data, despite another parent having given written consent

5.4 Consent can be withdrawn from a biometric system at any time by contacting the relevant school.

6. Alternative Provision

6.1 For students where the Trust cannot process biometric data for use in automatic biometric recognition systems (5.3), the Trust will provide alternative arrangements for affected services.

6.2 Alternative arrangements will ensure no student suffers any disadvantage or difficulty in accessing affected services as a result of not participating in an automatic biometric recognition system.

7. Supporting Information

7.1 DfE, 'Protection of biometric information of children in schools and colleges: Advices for proprietors, governing bodies, head teachers, principals and school and college staff': https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/692116/Protection_of_Biometric_Information.pdf

7.2 ICO, 'What is special category data?': https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/#scd4