CARLTON
ACADEMY TRUST

Carlton Academy Trust
Protection of Biometric Information Policy

Signed on behalf of Trustees:	**Roger Butterfield**
Date:	**August 2023**
Next Review Date:	**August 2024**

Glossary

GDPR: General Data Protection Regulation
ICO: Information Commissioners Office
Parents: Umbrella term also including carers

Policy Statement

The Trust is committed to protecting all personal data it processes. This includes biometric data which is collected in accordance with the UK GDPR (2018), the Data Protection, Privacy and Electronic Communications Regulations (2020), and the requirements in sections 26 to 28 of the Protection of Freedoms Act (2012).

Definition

Biometric data is information about an individual's physical characteristics that can be used to identify that person. It includes fingerprints, facial shape, retina and iris patterns, and hand measurements. The ICO considers all biometric information to be personal data as defined by GDPR and must be obtained, used, and stored in accordance with its guidelines.

Automated biometric recognition systems measure an individual's physical characteristics, then compares these against stored biometric information to recognise or identify the individual.

Data Processing

Data processing is either:

- Obtaining, recording, or holding data

Or

- Carrying out any operation/s on data, including disclosing, deleting, organising, or altering it.

A biometric system processes data when:

- Recording students' biometric data, such as taking measurements from a fingerprint scanner.
- Storing students' biometric information on a database.
- Using stored data as part of an electronic process, such as comparing it with biometric information stored on a database to identify or recognise students.

Consent

Prior to any biometric recognition system being used, the school must gain consent from all relevant parties. For students this requires written consent from a parent, as shown in Appendix 1.

Consent is valid until withdrawn by a parent or the student. Parents must make a withdrawal request in writing, but students can do this verbally. When a student or staff member leaves a school, their biometric data is securely removed from the biometric system.

Appendix One: Consent Forms

Parent Notification and Consent Form

Student Consent

Name: ……..……

Please sign below if you consent to the school taking and using information from your child's fingerprint as part of an automated biometric recognition system. This will be used for

…….....

In signing this form, you are authorising the school to use your son/daughter's biometric information for this purpose until they leave the school or cease to use the system.

If you wish to withdraw your consent in the future, this can be done by writing to the Head of School. Once your child ceases to use the system, their biometric information will be securely deleted.

I give consent to information from the fingerprint of my child being taken and used by the school for use as part of a biometric recognition system.

Parent Name: …….

Signature…… **Date** ……

Staff Consent

Name: ……

Please sign below if you consent to the school/trust taking and using information from your fingerprint as part of an automated biometric recognition system. This will be used for

…….....

In signing this form, you are authorising the school/trust to use your biometric information for this purpose until you either leave the school/trust or you cease to use the system.

You can withdraw your consent at any time. This must be done in writing to the Head of School. Once you cease to use the biometric recognition system, your biometric information will be securely deleted.

Having read the above guidance information, I give consent to information from my fingerprint being taken and used by the School/Trust for use as part of a biometric recognition system.

Signature…… **Date** ……