



St Augustine's CE High School

Biometric Data Policy

We are committed to using biometric data responsibly to enhance the efficiency and security of our school systems, while safeguarding the personal information of students and staff. Our goal is to create a secure, inclusive environment where technology serves to support learning and safety with the utmost consideration for individual rights and privacy.

| | | |
|----------------------------|-----------------|---------------------------|
| Approved by: | Governing Body | Date: January 2025 |
| Last reviewed on: | 20 January 2024 | |
| Next review due by: | January 2026 | |

We are committed to creating a safe, secure and supportive learning environment for all students, staff and visitors. CCTV technology is used responsibly and respectfully to safeguard the well-being of everyone on our premises.



What do we mean by biometric data?

Biometric data means personal information resulting from specific technical processing relating to the individual's physical, psychological or behavioural characteristics which allow or confirm the unique identification of that person, such as facial images, voice recognition or fingerprints. (DfE, July 2022)

What does process data mean?

'Processing' of biometric data 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 pupil/students' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner
- storing pupil/students' 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 pupil/students'

What does the law say?

Under the Protection of Freedoms Act 2012, we are required to notify each parent/ carer of a child and obtain the written consent of at least one parent before being able to use a child's biometric information for an automated system.

The parent/ carer may object at any time to the processing of the information.

A pupil's or student's objection or refusal, overrides any parental consent to the processing, therefore any biometric data must not be processed.

The school should endeavour to store biometric data securely to prevent any unauthorised or unlawful use.

The school should not keep biometric data for longer than it is needed meaning that a school or college should destroy a pupil's/student's biometric data if, for whatever reason, they no longer use the system including when leaving the school or college, where a parent withdraws consent or the pupil/student either objects or withdraws consent.

The school should endeavour to ensure that biometric data is used only for the purposes for which they are obtained and that such data are not unlawfully disclosed to third parties



At St Augustine's

We seek consent for your child's biometric information to be used for the purpose of providing your child with access to the cashless catering system. See Addendum I

Other policies

This Biometric Data Policy is linked to the school's:

- Freedom of Information Publication Scheme
- Online and E-Safety Policy
- ICT User Agreements
- Email Use Policy
- Document Retention Policy
- Breach Management Policy
- Asset Management Recording Policy
- Disaster Recovery/Business Continuity Planning and Risk Register.
- Safeguarding and Child Protection Policy

In the event where the school does not have a named policy, as stated within this Policy, advice and guidance will be sought from the Policies used by the LDBS Academies Trust, as this Policy is based on their model.



FAITH



HOPE



LOVE



GROWTH

Addendum I

**STUDENTS/PARENTS/GUARDIAN CONSENT TO PROCESS
BIOMETRIC INFORMATION FOR ACCESS TO CASHLESS CATERING SYSTEM**

We are required seek your written consent under the General Data Protection Regulation 2018 (GDPR) to use your child's biometric information for purposes of cashless catering system. We have been using the biometric recognition system for a number of years, however, due to the new regulations, we require your consent to hold the data.

The biometric recognition system will take specific details of your child's fingerprint and map these into an encrypted format. This encrypted information is stored securely on the cashless catering server system.

- The school would like to take and use information from your child's fingerprint for the purpose of providing your child with access to the cashless catering systems.
- Written consent of at least one parent is required. Consent given by one parent will be overridden if the other parent objects in writing to the use of their child's biometric information.
- If you give consent but later change your mind, you can withdraw this consent. Please note that any consent, withdrawal of consent or objection from a parent or legal guardian must be in writing.
- The school asks that you discuss the biometric system with your child. If your child objects, the school cannot collect or use his/her biometric information.
- You are advised that PIN codes do not have the same level of security and it will be your child's responsibility to remember the code and keep it secure at all times.

I confirm that I have read and understood the above and give the consent for the school to use my child's biometric data as described above.

Student Name: _____ **Form Group:** _____

Parent/Carer Name: _____ **Signature** _____ **Date:** _____



FAITH



HOPE



LOVE



GROWTH