



Fulston Manor Academies Trust

Biometric Data Policy

**Fulston Manor School
South Avenue Primary School**

Version (Date):

July 2026

Review (Date):

July 2027

Member of Staff Responsible:

Mrs M Smith

This is the Biometric Data Policy of Fulston Manor Academies Trust (trust) and is published in accordance with the Protection of Freedoms Act 2012 and the Data Protection Act 2018 (DPA). It sets out how such data will be used by the trust.

Biometric information

Biometric information is information about a person's physical or behavioural characteristics that can be used to identify them, for example, information from their fingerprint. It is defined in the Data Protection Act (DPA) as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual, which allows or confirms the unique identification of that individual, such as facial images or dactyloscopy data."

Scope

Biometric information may be used for a range of applications and services. At present, the trust's use of biometric information is limited to facilitating the administration of school meals. This system takes measurements of a person's fingerprints and converts these measurements into a template to be stored on our system. An image of the fingerprint is not stored. The template (i.e. measurements taken from the fingerprint) is what will be used to permit access to the service.

The trust may review and improve its administrative procedures or working practices in the future. If the solution involves the use of biometric information, the trust will contact parents and guardians and seek their consent for the use of biometric information for any new and additional purpose to that already in place.

Legal Basis

The Protection of Freedoms Act 2012 (sections 26 to 28) places specific requirements on schools and colleges when using personal information, such as biometric information, about students for the purposes of an automated biometric recognition system.

For the use of the biometric system, the trust relies on Article 6(1)(a) UK GDPR/ DPA 2018 consent as the lawful basis for processing and Article 9(2)(a) UK GDPR/DPA 2018 explicit consent as the special category condition. For pupils under 18, the trust will also comply with sections 26 to 28 of the Protection of Freedoms Act 2012, including parental notification, written consent requirements, the pupil's right to refuse or withdraw, and the provision of a reasonable alternative.

Our Procedures

Under the UK GDPR / DPA 2018, the trust must seek specific consent from a parent, student, member of staff or volunteer, including a Trust Member or Director, if it would be beneficial for the trust, school or the individual to provide such information.

A student may object or refuse to participate (or to continue to participate) in activities that involve the processing of their biometric data, and this objection or refusal overrides any parental consent to the processing.

A member of our administrative team contacts each parent or legal guardian by email seeking their written consent for their child to provide their biometric profile. This involves the pupil having their fingerprints taken by a digital reader operated by a trained member of staff. The data relating to each pupil is stored securely on the trust's server, enabling automated verification and payment via a third party (BioStore).

If consent is refused, the trust will ensure that the student's biometric data is not taken or used as part of a biometric recognition system. If consent is withdrawn after data has been taken, the data will be destroyed following withdrawal of consent.

Compliance Safeguards

The trust's use of biometric information is strictly limited to the administration of school meals and cashless catering, including confirming that meals are supplied to the correct person. Biometric

information will not be used for attendance, behaviour monitoring, safeguarding, access control, profiling, or any other purpose unless a new assessment is completed, parents and pupils are informed, and any required consent is obtained.

Biometric data used for the purpose of uniquely identifying an individual is special category personal data. The trust will only process such data where it has a lawful basis under UK GDPR / DPA 2018 and a relevant special category condition, which will normally include explicit written consent. Consent may be withdrawn at any time. Where a pupil objects or refuses to participate, that objection or refusal will be respected and will override any parental consent.

Before using, changing or extending any biometric recognition system, the trust will complete and maintain a Data Protection Impact Assessment. The assessment will consider the necessity and proportionality of the processing, risks to pupils and other users, security measures, alternative arrangements, supplier controls, and whether the system remains appropriate for its stated purpose. Alternative arrangements will be available for any pupil who does not use the biometric system. These arrangements will provide access to meals in a fair, practical and non-discriminatory way. Pupils who do not use biometrics will not be disadvantaged, delayed, identified publicly, or treated differently because they access meals through an alternative method.

Biometric templates will be retained only for as long as necessary for the administration of school meals. The trust will arrange for biometric data to be deleted when consent is withdrawn, when a pupil leaves the school, when the system is no longer required, or when the data is otherwise no longer necessary for the stated purpose. Where a third-party supplier processes the data, the trust will require appropriate confirmation that deletion has taken place.

Any third-party supplier involved in providing or supporting the biometric system, including BioStore, must process biometric data only on the trust's documented instructions and only for the agreed school meal's purpose. The trust will ensure that appropriate contractual and security controls are in place, including confidentiality obligations, access restrictions, secure storage, breach notification requirements and deletion or return of data at the end of the service.

The system and any alternative arrangements must protect the confidentiality of pupils entitled to free school meals. Staff should ensure that use of the catering system does not make a pupil's free school meal status visible to other pupils or unauthorised persons.

This Policy should be read in conjunction with the trust's Privacy Policy and Data Protection Policy.

Further information and guidance

"Protection of children's biometric information in schools: Guidance for schools, sixth-form colleges, 16 to 19 academies and further education institutions wishing to use automated biometric recognition systems."

<https://www.gov.uk/government/publications/protection-of-biometric-information-of-children-in-schools>

July 2026