We are an ambitious and inclusive Trust of Trusts strengthening communities through excellent education.

Biometrics Policy

Responsibility for approval: Senior Executive
Date of Approval : November 2026
Next review : October to December 2027

Contents Page

1.0 Policy Statement

2.0 Scope and Purpose

3.0 Definition

4.0 Legal Framework

5.0 What is Biometric Data?

6.0 What is an Automated Biometric Recognition System?

7.0 Authorised Use of Biometric Data

8.0 Consent and Withdrawal of Consent

8.1 Consent for Pupils

8.2 Consent for Staff

9.0 Retention and Deletion of Biometric Data

10.0 Storage and Security of Biometric Data

11.0 Reasonable Alternatives

12.0 Responsibilities and Review

Appendix 1 – Parent/Carer Biometric Consent Form

Appendix 2 – Staff Biometric Consent Form

Document Review and Approval

1.0 Policy Statement

- We are an ambitious and inclusive Trust of schools strengthening our communities through excellent education. We are committed to providing excellent education for every child, every day, and aim to strengthen and work with our communities to ensure confident compliance.

2.0 Scope and Purpose

- This policy is based on our values of collaboration and building trust; it sets out the Trust's framework for the lawful, fair and transparent use of biometric data across its schools.
- This policy applies to pupils and staff whose biometric data is processed by the Trust or one of its schools.

3.0 Definition

- For the purpose of this document, Ted Wragg Multi Academy Trust is referred to as Ted Wragg Trust, TWT or the Trust.

4.0 Legal Framework

- This policy will be published on the Trust website, included in the Trust's Policy Monitoring Schedule and forms part of the Data Protection Policy Page.
- This policy is informed by sections 26 to 28 of the Protection of Freedoms Act 2012, the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR).

5.0 What is Biometric Data?

- Biometric data means personal information about an individual's physical or behavioural characteristics that can be used to identify that person; this can include fingerprints, facial shape, retina and iris patterns and hand measurements.
- All biometric data used for the purpose of uniquely identifying an individual is special category data under the UK GDPR. It is more sensitive and requires additional protection because its misuse could create significant risks to a person's fundamental rights and freedoms.
- The Trust has carried out, and will carry out where a new use or material change is proposed, a Data Protection Impact Assessment (DPIA) to evaluate whether the use of biometric data is necessary and proportionate to the legitimate objectives being pursued.
- The outcome of the DPIA will inform each school's use of biometrics and the controls set out in this policy.

6.0 What is an Automated Biometric Recognition System?

- An automated biometric recognition system uses technology to measure an individual's physical or behavioural characteristics through equipment that operates automatically. Information from the individual is automatically compared with biometric information stored in the system to determine whether there is a match and to recognise or identify the individual.

7.0 Authorised Use of Biometric Data

- Processing biometric information includes obtaining, recording or holding the data, or carrying out any operation or set of operations on it, including disclosing, deleting, organising or altering it.
- As biometric data used for unique identification is special category data, a school must identify both a lawful basis for processing personal data and a separate condition for processing special category data. The Trust's schools rely on explicit consent for the uses covered by this policy.

- At the time of review, All Saints Church of England Academy, Exmouth Community College, Honiton Community College, Sidmouth College and Tor Bridge High process biometric data to support their canteen and lunch facilities. This arrangement, the current systems used and the schools included in this list must be confirmed before approval.
- The intended benefits are improved efficiency, reduced reliance on swipe cards and cash, and support for pupil safeguarding. Each school must be able to demonstrate that the use remains necessary and proportionate.
- Facial recognition technology is likely to present a high data protection risk. It must not be introduced unless a DPIA has been completed before use, parents and pupils have been consulted, explicit consent has been obtained, and a reasonable non-biometric alternative is available.

8.0 Consent and Withdrawal of Consent

- Schools will not process biometric information without the relevant explicit consent.

8.1 Consent for Pupils

- When obtaining consent for a pupil, both parents will be notified that the school intends to use and process their child's biometric information. Written consent is required from only one parent under the Protection of Freedoms Act 2012, provided that no parent objects to the processing.
- If either parent objects, the school will not process the child's biometric data and will provide a reasonable alternative that allows access to the same service.
- A pupil may also object to the processing of their biometric data. If a pupil objects, the school will not process or continue to process their biometric data, irrespective of whether a parent has provided consent.
- Where a pupil objects or withdraws consent, the school will inform the parent or carer where it is appropriate and lawful to do so, taking account of the pupil's age, understanding and circumstances.
- Parents and pupils may object at a later stage. A parent may withdraw consent by contacting dataprotection@tedwraggtrust.co.uk and asking the school to stop using their child's biometric data.
- A pupil does not need to withdraw consent in writing and may tell an appropriate member of school staff. The existing arrangement that pupils notify school reception must be confirmed by each school.
- Consent will last while the pupil attends the school unless it is withdrawn or the purpose for processing ends.
- Where a child is looked after and is subject to a care order in favour of a local authority, or is accommodated by a local authority within section 22(1) of the Children Act 1989, the school will establish who must be notified and who may provide consent in the child's circumstances.

8.2 Consent for Staff

- Schools will obtain explicit consent from staff before processing their biometric data. If a staff member objects or withdraws consent, the school will stop processing the biometric data and provide a reasonable alternative.
- A staff member who wishes the school to stop using their biometric data should write to the Headteacher. This local contact arrangement and the alternative offered to staff must be confirmed before approval.
- Consent will last while the staff member remains employed by the school unless it is withdrawn or the purpose for processing ends.

9.0 Retention and Deletion of Biometric Data

- Biometric data will be retained only for as long as valid consent remains in place and the data is required for the stated purpose.

- The current Trust arrangement is that biometric data will be deleted from the school's system within seven days when a pupil or staff member leaves, ceases to use the system, or consent is withdrawn. The Trust and each relevant supplier must confirm that this period is operationally achievable and reflected in the applicable privacy information and consent wording.
- Deletion must include the biometric template or other biometric information held within the school-controlled system and, where applicable, deletion by the supplier in accordance with the Trust's instructions.

10.0 Storage and Security of Biometric Data

- Biometric data will be kept securely, with appropriate technical and organisational measures to prevent unauthorised or unlawful access, use, alteration, disclosure, loss or destruction.
- Biometric data will be used only for the purpose for which it was obtained and will not be disclosed to third parties unless there is a lawful basis and appropriate safeguards are in place.
- Access will be limited to authorised personnel who require it for their role, and the Trust will ensure that relevant supplier arrangements are documented and reviewed.

11.0 Reasonable Alternatives

- A pupil or staff member who does not consent, or who withdraws consent, will not be disadvantaged. The school will provide a reasonable alternative that allows access to the same facilities or services without requiring biometric data.
- Each school must record and confirm the alternative available for each biometric system before the system is used or this policy is approved.

12.0 Responsibilities and Review

- Senior Executive is responsible for approval of this policy. The Trust Lead for Complaints and Compliance will coordinate the policy review and data protection assurance activity.
- Schools using biometric systems are responsible for confirming that consent records, pupil objections, reasonable alternatives, deletion arrangements, supplier controls and privacy information remain accurate and effective.
- This policy will be reviewed in accordance with the Trust's Policy Monitoring Schedule and earlier where there is a material change to the law, guidance, technology or manner in which biometric data is used.

Appendix 1 – Parent/Carer Biometric Consent Form

- This appendix must be retained only where the Trust's approved consent form is used. The final form must identify the school, the biometric system, the specific purpose, the reasonable alternative, the withdrawal contact and the confirmed deletion period.
- I consent to the school taking and using biometric information about my child as part of an automated biometric recognition system for the following purpose: [INSERT SPECIFIC PURPOSE].
- I understand that my child may object or refuse at any time, that I may withdraw my consent at any time, and that a reasonable alternative will be provided without disadvantage.
- Parent/carer name: .....
- Signature: ..... Date: .....
- Name of pupil: .....
- Please return this form to: [INSERT SCHOOL CONTACT].

Appendix 2 – Staff Biometric Consent Form

- This appendix must be retained only where the Trust's approved staff consent form is used. The final form must identify the school, biometric system, purpose, reasonable alternative, withdrawal contact and confirmed deletion period.
- I consent to the school taking and using my biometric information as part of an automated biometric recognition system for the following purpose: [INSERT SPECIFIC PURPOSE].
- I understand that I may withdraw my consent at any time and that a reasonable alternative will be provided without disadvantage.
- Staff name: .....
- Signature: ..... Date: .....
- Please return this form to: [INSERT SCHOOL CONTACT].