

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



Management of Information - Biometrics Policy

Responsibility for approval: Senior Executive
Approval date: November 2025
Next review: November to January 2027

Contents Page

Table of Contents

Contents Page.....	2
1.0 Policy Statement.....	3
2.0 Scope and Purpose.....	3
3.0 Definition.....	3
4.0 Legal Framework.....	3
5.0 What is Biometric Data?	3
6.0 What us an Automated Biometric Recognition System.....	3
7.0 Authorised usage of AI for staff	3
8.0 Consent and Withdrawal of Consent.....	4
9.0 Retention of Biometric Data	5
10.0 Storage of Biometric Data.....	5

1.0 Policy Statement

- 1.1 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

- 2.1 This policy is based on our values of collaboration and building trust; it sets out the Trust's framework to ensure compliance with the UK GDPR Data Protection Principles, its retention of personal data and in providing a right of access to official information in line with what is permitted by the Freedom of Information Act.

3.0 Definition

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

4.0 Legal Framework

- 4.1 This Policy will be published the Trust website it will be published and will be included in the Trust's Policy Monitoring Schedule. It forms part of us [Management of Information Policy Suite](#)

5.0 What is Biometric Data?

- 5.1 Biometric data means personal information about an individual's physical or behavioural characteristics that can be used to identify that person; this can include their fingerprints, facial shape, retina and iris patterns and hand measurements.
- 5.2 All biometric data is considered to be special category data under the UK General Data Protection Regulation (UK GDPR). This means the data is more sensitive and requires additional protection as this type of data could create more significant risks to a person's fundamental rights and freedoms.
- 5.3 This policy complies with The Protection of Freedoms Act 2012 (sections 26 to 28), the Data Protection Act 2018 and the UK GDPR.
- 5.4 The Trust have and will carry out a Data Protection Impact Assessment with a view to evaluating whether the use of biometric data is a necessary and proportionate means of achieving the legitimate objectives set out below.
- 5.5 The result of the Data Protection Impact Assessment has informed the school's use of biometrics and the contents of this policy.

6.0 What is an Automated Biometric Recognition System

- 6.1 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 stored in the system to see if there is a match in order to recognise or identify the individual.

7.0 Authorised usage Biometric data

- 7.1 'Processing' of biometric information 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.

- 7.2 As biometric data is special category data; in order to lawfully process this data, the school must have a legal basis for processing personal data and a separate condition for processing special category data. When processing biometric data, Schools rely on explicit consent (which satisfies the fair processing conditions for personal data and special category data).
- 7.3 At the time of publishing, All Saints Church of England Academy, Exmouth Community College, Honiton Community College, Marine Academy Plymouth, Sidmouth College and Tor Bridge High all process biometric data as an aim to make significant improvements to their canteen and lunch facilities. This is to ensure efficiency, to do away with the need for swipe cards and cash being used, to safeguard the children.

8.0 Consent and Withdrawal of Consent

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

Consent for pupils

- 8.2 When obtaining consent for pupils, both parents will be notified that the school intends to use and process their child's biometric information. Schools only require written consent from one parent (in accordance with the Protection of Freedoms Act 2012), provided no parent objects to the processing.
- 8.3 If a parent objects to the processing, then Schools will not be permitted to use that child's biometric data and alternatives will be provided.
- 8.4 Children over 12 years of age may also object to the processing of their biometric data. If a child objects, Schools will not process or continue to process their biometric data, irrespective of whether the parent(s) has provided consent. In this instance, schools are obliged to inform the parents/carers that consent has been withdrawn by the pupil.
- 8.5 Where there is an objection, Schools will provide reasonable alternatives which will allow the child to access the same facilities that they would have had access to have their biometrics been used.
- 8.6 Pupils and parents can also object at a later stage to the use of their child's/their biometric data. Should a parent wish to withdraw their consent, they can do so by contacting the Trust at dataprotection@tedwraggtrust.co.uk requesting that the school no longer use their child's biometric data.
- 8.7 Pupils who wish for the school to stop using their biometric data do not have to put this in writing but should let school reception know.
- 8.8 The consent will last for the time period that your child attends the school (unless it is withdrawn).
- 8.9 Where a child is looked after and is subject to a care order in favour of the local authority or the local authority provides accommodation for the child within the definition of section 22(1) of the Children Act 1989, the school would not normally be required to notify or seek consent from the birth parents.

Consent for staff

- 8.10 Schools will seek consent of staff before processing their biometric data. If the staff member objects, the school will not process or continue to process the biometric data and will provide reasonable alternatives. Staff who wish for the school to stop using their biometric data should do so by writing to the Headteacher.
- 8.11 The consent will last for the time period that the staff member remains employed by the school (unless it is withdrawn).

9.0 Retention of Biometric Data

- 9.1 Biometric data will be stored by Schools for as long as consent is provided (and not withdrawn).
- 9.2 Once a pupil or staff member leaves, the biometric data will be deleted from the school system within 7 days of them leaving.

10.0 Storage of Biometric Data

- 10.1 At the point that consent is withdrawn, the school will take steps to delete their biometric data from the system within 7 days of the request.
- 10.2 Biometric data will be kept securely, and systems will be put in place to prevent any unauthorised or unlawful access/use.
- 10.3 The biometric data is only used for the purposes for which it was obtained, and such data will not be unlawfully disclosed to third parties.