



Biometric Data Policy

Author	Cheryl Campbell
Created	September 2021
Reviewed:	September 2025
Governors Committee:	Resources
Agreed by Governors:	October 2025
Frequency of Review	Annually
Review Date:	September 2026

ETHICAL LEADERSHIP

1. Thomas Tallis School Plan aims are:

1	Powerful Knowledge for all
2	Tallis Praxis
3	The Tallis Experience
4	Learning Behaviours to Build a Strong Community
5	A Model for a Better World

As part of the aims Thomas Tallis School has adopted the *Framework for Ethical Leadership in Education*. This means that we try to behave in a principled and correct manner in everything we do.

Schools and colleges serve children and young people and help them grow into fulfilled and valued citizens. As role models for the young, how we behave as leaders is as important as what we do. We therefore behave with **selflessness, integrity, objectivity, accountability, openness, honesty and leadership**. We demonstrate **trust, wisdom, kindness, justice, service, courage and optimism**.

What is Biometric Data?

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.
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 more protection and this type of data could create more significant risks to a person's fundamental rights and freedoms.
3. This policy complies with The Protection of Freedoms Act 2012 (section 26 – 28), the Data Protection Act 2018 and the UK GDPR).
4. Schools that use pupils' biometric data must treat the data collected with appropriate care and must comply with the data protection principles as set out in the UK General Data Protection Regulation 2018.
5. The Information Commissioner considers all biometric information to be personal data as defined by the UK General Data Protection Regulation 2018; this means that it must be obtained, used and stored in accordance with the Regulation.
6. Personal data used as part of an automated biometric recognition system must also comply with the additional requirements in sections 26 to 28 of the Protection of Freedoms Act 2012.
7. The Protection of Freedoms Act 2012 includes provisions which relate to the use of biometric data in schools when used as part of an automated biometric recognition system.
8. Schools must ensure that the parent/carer of each pupil is informed of the intention to use the pupil's biometric data as part of an automated biometric recognition system. Parents/carers must be advised that alternative methods to biometric scanning are available for processing identity if required.
9. The written consent of the parent/carer or the pupil, where the pupil is deemed to have the capacity to consent, must be obtained before the data is taken from the pupil and processed within the biometric recognition system. In no circumstances can a pupil's biometric data be processed without written consent - see Appendix A
10. Schools must not process the biometric data of a pupil where:
 - a) the pupil (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data;
 - b) a parent or pupil has not consented in writing to the processing; or

- c) a parent or pupil has objected in writing to such processing, even if another parent has given written consent.
11. Schools must provide reasonable alternative means of accessing the services to those pupils who will not be using an automated biometric recognition system.

Biometric Data and Processing

What Is an Automated Biometric Recognition System?

12. 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.

The legal requirements under UK GDPR

13. '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.
14. An automated biometric recognition system processes data when:
- a) recording pupils' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner;
 - b) storing pupils' biometric information on a database system; or
 - c) 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 pupils.
15. 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, the school rely on explicit consent (which satisfies the fair processing conditions for personal data and special category data). Consent is obtained using the consent form(s) in the attached appendix
16. The school process biometric data as an aim to make significant improvements to our canteen and lunch facilities or for pupils to sign in/move around the school. This is to do away with the need for swipe cards and cash being used.

Who Is Able to Give Consent?

17. The Data Protection Act gives pupils rights over their own data when they are considered to have adequate capacity to understand. Most pupils will reach this level of understanding at around age 13.
18. For this reason, for most pupils in a secondary school, it will normally be up to the individual pupil to decide whether or not to provide biometric data. Where the school considers that the pupil does not have the capacity, or they are under the age of 13, parents/carers will be asked to provide written consent.

Consent for Pupils

19. When obtaining consent for pupils, both parents will be notified that the school intend to use and process their child's biometric information. The school only require written consent from one parent (in accordance with the Protection of Freedoms Act 2012), provided no parent objects to the processing.
20. If a parent objects to the processing, then the school will not be permitted to use that child's biometric data and alternatives will be provided.
21. The child may also object to the processing of their biometric data. If a child objects, the school will not process or continue to process their biometric data, irrespective of whether consent has been provided by the parent(s).
22. Where there is an objection, the school will provide reasonable alternatives which will allow the child to access the same facilities that they would have had access to had their biometrics been used.
23. 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 writing to the school at GDPR@thomastallis.org.uk requesting that the school no longer use their child's biometric data.
24. Pupils who wish for the school to stop using their biometric data do not have to put this in writing but should let Mrs Shaldas, Deputy Head, know.
25. The consent will last for the time period that your child attends the school (unless it is withdrawn).

Consent for staff

26. The school 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 Chief Operating Officer.

27. The consent will last for the time period that the staff member remains employed by the school (unless it is withdrawn).

Alternative to Biometric

28. The school will provide an alternative to biometric scanning for any parent/pupil objecting to the processing of biometric data.

Length of Consent

29. The original written consent is valid until such time as it is withdrawn. However, it can be overridden, at any time either parent/carer or the pupil themselves objects to the processing (subject to the parent's/carer's objection being in writing). When the student leaves the school, their biometric data will be securely removed from the school's biometric recognition system.

Retention of Biometric Data

30. Biometric data will be stored by the school for as long as consent is provided (and not withdrawn).

31. Once a pupil [or staff member] leaves, the biometric data will be deleted from the school's system no later than 1 month.

32. At the point that consent is withdrawn, the school will take steps to delete their biometric data from the system and no later than 72 hours.

Storage of Biometric Data

33. Biometric data will be kept securely and systems will be put in place to prevent any unauthorised or unlawful access/use.

34. 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.

Monitoring and Review of This Policy

35. The Governing Body shall be responsible for reviewing this policy from time to time to ensure that it meets legal requirements and reflects best practice

Appendix 1

Dear Parents and Carers

Biometric Data

At Thomas Tallis we operate a biometric scanning payment system for our catering service which works very successfully for us. We believe that it speeds up the food service and reduces the risks of children carrying cash. We also use the biometric scanning system for printing and photocopying, the library system and for late registration.

How do we use this information?

You may know that the system uses the thumb print of each student, through software which calculates a secure digital ID from that image. It is the number itself which is stored for personal identification NOT the thumb print. The stored information is kept on a secure server in school, is no use to any other system.

Consent

In line with the Protection of Freedoms Act 2012, we have to obtain written consent from a parent or carer for each pupil in this system. Without written consent your child will not be able to use his or her thumbprint, so please complete the attached authorisation form.

If you object, or do not give written consent to the use of biometric data for this purpose, then we will need to provide your child with a 4-digit PIN to be manually entered each time your child uses the system. We believe that this is slower and much less secure.

Please do not hesitate to contact us if you would like more details. Our Operations Manager can answer your questions.

Yours sincerely

Steve Parsons
Headteacher

Biometric Data - please tick the box of your preference:

- I give my consent for Thomas Tallis School to take my child's thumb print.
- I do not give my consent for Thomas Tallis School to take and store this information and request that he or she is given a 4-digit PIN.

Pupil's Name:

Parent's or Carer's Signature: Date:

End of document