Biometric Data Policy

Approved by:	Trust Board	**Date:**	October 2023
Next review due by:	Autumn 2025		

Document Control

Issue No	Date	Amended by	Summary of Changes
1		Holly Walker	New policy; removed from combined DP and FOI policy

Authorisation (Responsible Owner)

Name	Role	Approval Date

Approval (Accountable Owner)

Name	Role	Approval Date

Distribution List – Once authorised (Informed)

Name	
Headteachers	
SIROs/DPLs	
	For uploading to Trust website

Review Period (at least annually or whenever statutory guidance changes)

Date Document Reviewed	By Whom
	Holly Walker

1. Policy Aim

1.1. Unity Schools Partnership and the schools therein ("The Trust") is committed to protecting the personal data of all its pupils and staff, this includes any biometric data we collect and process. We collect and process biometric data in accordance with relevant legislation and guidance to ensure the data and the rights of individuals are protected. This policy outlines the procedure that the Trust follows when collecting and processing biometric data.

1.2. This policy is written with due regard to all relevant legislation and guidance including, but not limited to, the following:

1.2.1. Protection of Freedoms Act 2012

1.2.2. Data Protection Act 2018

1.2.3. General Data Protection Regulations (GDPR)

1.2.4. DfE (2018) 'Protection of biometric information of children in schools and colleges'

1.3. This policy operates in conjunction with the following Trust policies:

1.3.1. Data Protection Policy

1.3.2. Records Retention Policy

2. Defintions

2.1. Biometric data: Personal information about an individual's physical or behavioural characteristics that can be used to identify that person, including their fingerprints, facial shape, retina and iris patterns, and hand measurements.

2.2. Automated biometric recognition system: A system 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.

2.3. Processing biometric data: Processing biometric data includes obtaining, recording or holding the data or carrying out any operation on the data including disclosing it, deleting it, organising it or altering it. An automated biometric recognition system processes data when:

- Recording pupils' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner.
- Storing pupils' biometric information on a database.
- Using pupils' biometric data as part of an electronic process, e.g. by comparing it with biometric information stored on a database to identify or recognise pupils.

2.4 Special category data: Personal data which the GDPR says is more sensitive, and so needs more protection – where biometric data is used for identification purposes, it is considered special category data. More information can be found in our Data Protection policy.

3. Data protection principles

3.1. The Trust processes all personal data, including biometric data, in accordance with the key principles set out in the GDPR, as set out in our Data Protection policy.

3.2. As the data controller, the school is responsible for being able to demonstrate its compliance with the provisions outlined below by ensuring biometric data is:

- Processed lawfully, fairly and in a transparent manner.
- Only collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date, and that reasonable steps are taken to ensure inaccurate information is rectified or erased.

- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Processed in a manner that ensures appropriate security of the information, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4. Notification and consent

4.1. Please note that the obligation to obtain consent for the processing of biometric information of children under the age of 18 is not imposed by the Data Protection Act 2018 or the GDPR. Instead, the consent requirements for biometric information is imposed by section 26 of the Protection of Freedoms Act 2012.

4.2. Where the school uses pupils' biometric data as part of an automated biometric recognition system (for example, using pupils' fingerprints to receive school dinners instead of paying with cash), the school will comply with the requirements of the Protection of Freedoms Act 2012.

4.3. Prior to any biometric recognition system being put in place or processing a pupil's biometric data, the school will send the pupil's parents a Parental Notification and Consent Form for the use of Biometric Data.

4.4. Written consent will be sought from at least one parent of the pupil before the school collect or use a pupil's biometric data.

4.5. The name and contact details of the pupil's parents will be taken from the school's admission registers.

4.6. Where the name of only one parent is included on the admissions register, the Head teacher will consider whether any reasonable steps can or should be taken to ascertain the details of the other parent.

4.7. The school does not need to notify a particular parent or seek their consent if it is satisfied that:

- The parent cannot be found, for example, their whereabouts or identity is not known.
- The parent lacks the mental capacity to object or consent.
- The welfare of the pupil requires that a particular parent is not contacted, for example, where a pupil has been separated from an abusive parent who must not be informed of the pupil's whereabouts.
- It is otherwise not reasonably practicable for a particular parent to be notified or for their consent to be obtained.
- Where neither parent of a pupil can be notified for any of the reasons above, consent will be sought from the following individuals or agencies as appropriate:
- If a pupil is being 'looked after' by the LA or is accommodated or maintained by a voluntary organisation, the LA or voluntary organisation will be notified and their written consent obtained.

4.8. If the above does not apply, then notification will be sent to all those caring for the pupil and written consent will be obtained from at least one carer before the pupil's biometric data can be processed.

4.9. Notification sent to parents and other appropriate individuals or agencies will include information regarding the following:

- Details about the type of biometric information to be taken.
- How the data will be used.
- The parent's and the pupil's right to refuse or withdraw their consent.
- The school's duty to provide reasonable alternative arrangements for those pupils whose information cannot be processed.
- The school will not process the biometric data of a pupil under the age of 18 in the following circumstances:

- The pupil (verbally or non-verbally) objects or refuses to participate in the processing of their biometric data.
- No parent or carer has consented in writing to the processing.
- A parent has objected in writing to such processing, even if another parent has given written consent.

4.10. Parents and pupils can object to participation in the school's biometric system(s) or withdraw their consent at any time. Where this happens, any biometric data relating to the pupil that has already been captured will be deleted.

4.11. If a pupil objects or refuses to participate, or to continue to participate, in activities that involve the processing of their biometric data, the school will ensure that the pupil's biometric data is not taken or used as part of a biometric recognition system, irrespective of any consent given by the pupil's parent(s).

4.12. Pupils will be informed that they can object or refuse to allow their biometric data to be collected and used via a letter.

4.13. Where staff members or other adults use the biometric system(s), consent will be obtained from them before they use the system.

4.14. Staff and other adults can object to taking part in the biometric system(s) and can withdraw their consent at any time. Where this happens, any biometric data relating to the individual that has already been captured will be deleted.

4.15. Alternative arrangements will be provided to any individual that does not consent to take part in the biometric system(s), in line with section 5 of this policy.

5. Alternative arrangements

5.1. Parents, pupils, staff members and other relevant adults have the right to not take part in the biometric system(s).

5.2. Where an individual objects to taking part in the biometric system(s), reasonable alternative arrangements will be provided that allow the individual to access the relevant service, for example, where a biometric system uses pupil's fingerprints to pay for school meals, the pupil will be able to use cash for the transaction instead.

5.3. Alternative arrangements will not put the individual at any disadvantage or create difficulty in accessing the relevant service or result in any additional burden being placed on the individual (and the pupil's parents, where relevant).

6. Data retention

6.1. Biometric data will be managed and retained in line with the Trust's Records Retention Policy.

6.2. If an individual (or a pupil's parent, where relevant) withdraws their consent for their child's biometric data to be processed, it will be erased from the system.

7. Breaches

7.1. There are appropriate and robust security measures in place to protect the biometric data held by the school. These measures are detailed in the Trust's Data Protection Policy.

7.2. Any breach to the biometric system(s) will be dealt with in accordance with the Trust's Data Protection Policy.

8. Complaints

8.1. Trust complaints: All complaints must be made within 20 working days of the response being received and must detail the reasons for the appeal. A review will then be carried out internally by someone not involved in the original decision, usually this will be the Trust's Data Protection Officer.

8.2. Complaints can be made via dpo@unitysp.co.uk, via write to DPO, Unity Schools Partnership, Park Road, Haverhill, CB9 7YD

8.3. Information Commissioner's Office complaints: Complaints can also be made to the Information Commissioner's Office via https://ico.org.uk/concerns/ or via telephone 0303 123 1113 or write to Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

9. Contact

9.1. Any questions about this policy should be directed in the first instance to the Data Protection Officer via dpo@unitysp.co.uk