



Pate's Grammar School Policy

Protection of Biometric Information of Children in Schools and Colleges

**Approved by:
People & WellBeing
(sign off by FGB)**

Date: September 2021

**Last reviewed on:
September 2021**

**Next review due by:
September 2022**

Contents

1. Aims	2
2. Legislation and Guidance.....	2
3. Definitions.....	2
4. Roles and responsibilities.....	3
5. Data protection principles.....	3
6. Notification and consent.....	4
7. Alternative arrangements.....	5
8. Data retention	6
9. Breaches	6
10. Monitoring and review.....	6

1. Aims

Pate's Grammar School uses a biometric system (from Biostore) for paying for purchases in the refectory, printing, photocopying and scanning, as well as access to the school buildings. This policy is to confirm our approach to the use of biometric data.

Fingerprint images are not stored by the system (instead, a set of coordinates is translated into a string of letters/numbers and encrypted). The encryption method used by the system is a high level, industry standard method. The data held could not be used to recreate a fingerprint image, nor could it be used in a forensic investigation. The School offers an opportunity to opt out for those students who, upon consideration, feel that they would rather not have their biometric data recorded

Pate's Grammar School 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 the academies follow when collecting and processing biometric data.

2. Legislation and Guidance

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- [Protection of Freedoms Act 2012](#)
- [Data Protection Act 2018 o General Data Protection Regulation \(GDPR\)](#)
- [DfE \(2018\) 'Protection of biometric information of children in schools and colleges'](#)

3. Definitions

3.1 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.

3.2 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 to recognise or identify the individual.

3.3 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, e.g., 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.

3.4. 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.

4. Roles and responsibilities

4.1 The People & Wellbeing Committee is responsible for reviewing this policy on an annual basis.

4.2 The Head Master is responsible for ensuring the provisions in this policy are implemented consistently.

4.3 The Data Protection Officer (DPO) is responsible for:

- monitoring the Trust's compliance with data protection legislation in relation to the use of biometric data;
- advising on when it is necessary to undertake a data protection impact assessment (DPIA) in relation to the school's biometric system(s);
- being the first point of contact for the ICO and for individuals whose data is processed by the school and connected third parties.

5. Data protection principles

The school processes all personal data, including biometric data, in accordance with the key principles set out in the GDPR. The school ensures 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.

As the data controller, the school is responsible for being able to demonstrate its compliance with the provisions outlined above.

6. Notification and consent

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](#).

Where academies use pupils' biometric data as part of an automated biometric recognition system (eg using pupils' fingerprints to receive school dinners instead of paying with cash), the academy will comply with the requirements of the [Protection of Freedoms Act 2012](#). 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/carers a Parental Notification and a link for them to consent to the use of Biometric Data.

Consent will be sought from at least one parent/carer of the pupil before the academy collects or uses a pupil's biometric data.

6.1 The name and contact details of the pupil's parents/carers will be taken from the school's admission register.

6.2 Where the name of only one parent is included on the admissions register, the Head Master will consider whether any reasonable steps can or should be taken to ascertain the details of the other parent. The academy does not need to notify a particular parent/carer or seek their consent if it is satisfied that:

- the parent cannot be found, e.g. their whereabouts or identity is not known;
- the parent/carer lacks the mental capacity to object or consent;
- the welfare of the pupil requires that a particular parent/carer is not contacted, e.g. 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/carer to be notified or for their consent to be obtained.

6.3 Where neither parent of a pupil can be notified for any of the reasons set out in 6.6 (below), 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;
- 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.

6.4 Notification sent to parents/carers 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/carer'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.

6.5 The academy 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.

6.6 Parents/carers and pupils can object to participation in the academy'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.

6.7 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).

6.8 Pupils will be informed that they can object or refuse to allow their biometric data to be collected and used.

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

6.10 Staff and other adults can object to taking part in the school's 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.

6.11 Alternative arrangements will be provided to any individual that does not consent to take part in the school's biometric system(s), in line with section 6 of this policy.

7. Alternative arrangements

7.1 Parents/carers, pupils, staff members and other relevant adults have the right to not take part in the school's biometric system(s).

7.2 Where an individual objects to taking part in the school's 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 pupils' fingerprints to pay for school meals, the school's third party will provide the parent/carer with a fob.

7.3 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/carers, where relevant).

8. Data retention

8.1 Biometric data will be managed and retained in line with the Trust's records management policy.

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

8.3 when a student leaves the school, their data will be deleted.

9. Breaches

9.1 There are appropriate and robust security measures in place to protect the biometric data held by the Trust.

9.2 Any breach to the academy's biometric system(s) will be dealt with by the school and DPO.

10. Monitoring and review

10.1 The Protection of Biometric information Policy will be reviewed by the People & Wellbeing Committee annually.

10.2 Any material changes made to this policy will be communicated to all staff, parents/carers and pupils.