Ashton Community Science College

Pupil and Parent Biometrics Policy

Version Control

Named Owner:	Emily Loughran
Version Number:	1.00
Date Of Creation:	January 2026
Last Review:	
Next Scheduled Review:	January 2027
Overview of Amendments to this Version:	

Introduction

Ashton Community Science College ("the school") uses biometric recognition technology to support efficient, secure, and user friendly school operations. This policy explains how biometric data is collected, used, stored and protected and outlines the rights of parents and pupils under UK law.

The school is committed to processing biometric data lawfully, fairly and transparently in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the Protection of Freedoms Act 2012 (PoFA).

Legal Framework

The school complies with:

- Protection of freedoms act 2012 (sections 26-28).
- UK General Data Protection Regulation (UK GDPR).
- Data Protection Act 2018.
- Department of Educations (DfE) guidance on the use of biometric data in schools.

These laws require explicit consent, transparency, secure processing and respect for the rights of pupils and parents.

Lawful basis for processing

Under Article 6 UK GDPR, the school relies on:

- Article 6(1)(e) - Public task – Processing is necessary for schools to perform its public function of providing education and managing school operations.

As biometric data is special category data, the school also relies on:

- Article 9(2)(a) – Explicit consent. Biometric data will only be processed where explicit consent have been provided.

Consent is therefore a mandatory requirement for biometric processing in schools.

What is biometric data?

Biometric data refers to information about a person's unique physical or behavioural characteristics that can be used to identify them. In our school, this means fingerprint biometric templates and not actual fingerprint images.

What is a biometric template?

A biometric template is a mathematical representation of certain features of a fingerprint, not an image of the fingerprint itself. For example, when a pupil places their finger on the scanner, the system doesn't store a picture, instead it extracts a set of numerical values based on unique points in the fingerprint pattern. These values are then converted into a coded template. The template is then used to identity a pupil.

What is an automated biometric recognition system?

An automated biometric recognition system uses technology which measures an individuals physical or behavioural characteristics by using the equipment that operates automatically (ie 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 an individual.

What does data processing mean?

'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. An automated biometric recognition system processes data when:

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

Consent

The biometric system and the protection of freedom act 2012

The school uses a biometric fingerprint system in the catering facility. To comply with the above legislation, the school must have written confirmation in order for the biometric information for each child to be processed.

Parental notification

Before collecting or using biometric data the school will notify each parent with parental responsibility via Synergy. The notification will include, the purpose of the biometric data, how the data will be used, how long the data will be kept, how consent can be given or withdrawn and any parental responsibility requirements.

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

- The parent cannot be found.
- The parent lacks mental capacity to object or consent.
- The welfare of the student requires that a particular parent is not contacted.

Parental consent

Parental consent for the use of biometric data in schools must be explicit, informed, and freely given, as required by the Protection of Freedoms Act 2012 and UK GDPR. Before any biometric information is taken or used, the school must notify each parent with parental responsibility and obtain written consent from at least one parent, while also recognising that any parent may object, and an objection overrides consent.

Pupils' rights

Under the protection of Freedoms Act 2012, a pupil has the absolute right to refuse to participate in the biometric system. This right applies regardless of age and regardless of whether a parent has given consent. If a pupil's objects or withdraws, the school must provide an alternative method of identification. Where consent has not been obtained, pupils will be issued a pin number.

Withdrawal

Consent can be withdrawn at any time, by any pupil, parent or carer. To allow us to maintain an accurate record we ask that all withdrawals are emailed to enquiries@ashtoncsc.com and include the pupils full name, date of birth and the full name of the parent or carer withdrawing consent. Upon withdrawal, biometric data will be deleted in line with the policy retention plan.

Data retention and deletion

To comply with UK GDPR principles of storage limitation, biometric templates are retained only for as long as the individual uses the system. Once a pupil leaves, the Biometric data will be deleted from the school's system within 30 days.

Deleting is permanent and irreversible. If a pupil leaves school and returns later, they will need to provide new consent and complete the process again.

Data Security

The school takes appropriate technical and organisation measures to protect biometric data including. Our Biometric data is processed by our third party cashless catering system. All biometric data is stored locally on our server and not with the third-party catering system.

Third Party security

- All data is stored in a 256-bit advanced encryption standard (AES) environment.
- The data is processed in a cloud-based secure storage facility protected by biometric authentication and 27/7/365 surveillance.
- Access limited to authorised staff only.
- No paper copies of individuals data are held at anytime by the cashless catering system.

Schools' security

- Secure network – with protection against malware, spyware and ransomware.
- Access limited to authorised staff only.
- Software back up and replication completed by air gap cloud technology.
- All data stored within the UK.

Transferring Data Internationally

Where we transfer personal data to a country or territory outside the UK, we will do so in accordance with data protection law and ensure appropriate safeguards are in place.

Your rights:

How to access personal information that we hold about you

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. If you would like to make a request, please contact our data protection officer.

You also have the right to:

- Object to the use of your personal data if it would cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/.

Complaints

We take any complaints about our collection and use of personal information very seriously. If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/.

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this policy, please contact our data protection officer:

- Miss E Loughran, Data Manager, 01772 513002