Bassingbourn Community Primary School

Protection of biometric information of children in schools policy

This policy was ratified on:	30th April 2026
Implemented on:	30th April 2026
Review date:	April 2027

Purpose of the Policy

This policy sets out the legal duties and responsibilities of Bassingbourn Community Primary School should the school decide to use biometric information about pupils for the purposes of an automated biometric recognition system (for example, systems used for library borrowing, cashless catering, or access control).

The policy ensures compliance with:

- Sections 26–28 of the Protection of Freedoms Act 2012, and
- UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

The school recognises that the use of biometric data is a sensitive issue and is committed to protecting pupils' rights, privacy and welfare at all times.

Key Principles

- Biometric information is personal data and also special category personal data under UK GDPR.
- Biometric information will only be used where there is a clear educational or operational benefit.
- No pupil will be required to use biometric systems.
- Written parental consent and pupil agreement are essential.
- Pupils and parents have the right to refuse or withdraw consent at any time.
- Reasonable alternatives will always be provided without disadvantage.

What Is Biometric Information?

Biometric information is data which relates to a pupil's physical or behavioural characteristics and can be used to uniquely identify them. This may include:

- fingerprint data
- facial recognition data
- iris or retina patterns
- hand or palm measurements

When such data is used as part of an automated biometric recognition system, additional legal safeguards apply.

What Does "Processing" Mean?

Processing biometric information includes:

- obtaining the data (e.g. capturing a fingerprint or facial scan)

- recording or storing the data
- using the data to identify or recognise a pupil
- altering, deleting, or destroying the data

Biometric data will only be processed for the specific purpose for which consent has been obtained.

Legal Framework

1 Protection of Freedoms Act 2012

Under sections 26–28 of the Protection of Freedoms Act 2012:

- Schools must notify each parent of a pupil under 18 if they intend to use the pupil's biometric information.
- Written consent from at least one parent must be obtained before any biometric data is processed.
- Processing must not take place if:
    - the pupil objects or refuses to participate (verbally or non-verbally);
    - no parent has given written consent; or
    - any parent has objected in writing.

A pupil's objection always overrides parental consent.

2 Data Protection Law (UK GDPR and Data Protection Act 2018)

Biometric information is classified as special category personal data under UK GDPR. The school will:

- identify a lawful basis for processing under Article 6 UK GDPR;
- identify a specific condition for processing special category data under Article 9 UK GDPR;
- complete a Data Protection Impact Assessment (DPIA) before introducing or changing any biometric system;
- ensure all processing complies with the seven data protection principles:
    - Lawfulness, fairness and transparency
    - Purpose limitation
    - Data minimisation
    - Accuracy
    - Storage limitation

- Integrity and confidentiality (security)
- Accountability

Parental Notification and Consent

- Each parent will be informed in writing of the school's intention to use biometric information.
- Parents will be provided with clear information explaining:
  - the type of biometric data to be used;
  - how and why it will be used;
  - how long the data will be retained;
  - the right of parents and pupils to refuse or withdraw consent;
  - the availability of alternative arrangements.
- Written consent must be obtained from **at least one parent** before any biometric data is taken or used.

Where a parent cannot reasonably be contacted, or where contacting a particular parent would not be in the child's best interests, the school will rely on the lawful exemptions set out in the Protection of Freedoms Act 2012.

For looked-after children, the local authority (or relevant organisation) must be notified and give written consent.

The Pupil's Right to Refuse

- Pupils may object or refuse to participate in biometric processing at any time.
- Objections may be verbal or non-verbal.
- A pupil's objection **takes precedence over any parental consent**.

The school will ensure that pupils:

- are informed of their right to object in an age-appropriate way;
- understand that choosing not to participate will not result in any disadvantage.

Parents will also be informed of their child's right to refuse and encouraged to discuss this with their child.

Providing Alternatives

The school will provide reasonable alternative arrangements for pupils who do not use biometric systems, whether due to parental refusal or pupil objection.

Alternative arrangements will:

- enable equal access to all relevant services;
- not cause delay, embarrassment, or inconvenience;
- not place additional cost or burden on pupils or parents.

Data Security, Retention and Disposal

- Biometric data will be stored securely with appropriate technical and organisational safeguards.
- Access will be limited to authorised staff and approved system providers.
- Biometric data will not be retained for longer than necessary.
- Data will be securely deleted when:
    - the pupil stops using the system;
    - consent is withdrawn;
    - the pupil objects; or
    - the pupil leaves the school.

Biometric data will not be shared with third parties except where legally permitted and contractually safeguarded.

Roles and Responsibilities

- **Governing Body:**

Ensures this policy is in place, compliant with legislation, and reviewed regularly.

- **Headteacher:**

Responsible for implementation, ensuring consent procedures are followed, and staff awareness.

- **Data Protection Officer (DPO):**

Provides advice on GDPR compliance, DPIAs, and data security matters.

- **Staff:**

Must follow this policy and report any concerns or data incidents immediately.

Review and Monitoring

This policy will be reviewed annually or sooner if:

- legislation or DfE guidance changes;
- the school introduces or changes any biometric system.

This policy should be read in conjunction with the school's Data Protection Policy and Privacy Notices.