Benwick Primary School

Protection of Biometric Information Policy

School Name: Benwick Primary School

Date Agreed at FGB: 9.12.24

Next Review: 1/2/2026

Date shared with staff:

Statement of intent

Benwick Primary School is committed to protecting the personal data of all its pupils and staff, we DO NOT collect and process any biometric data.

1. Legal framework

1.1. 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
- General Data Protection Regulation (GDPR)
- DfE (2018) 'Protection of biometric information of children in schools and colleges'

1.2. This policy operates in conjunction with the following school policies:

- **Data Protection Policy**
- **Records Management Policy**
- **Data and E-Security Breach Prevention and Management Plan**

2. Definitions

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, 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.

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.

3. Legal framework

3.1. 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
- General Data Protection Regulation (GDPR)
- DfE (2018) 'Protection of biometric information of children in schools and colleges'

3.2. This policy operates in conjunction with the following school policies:

- **Data Protection Policy**
- **Records Management Policy**
- **Data and E-Security Breach Prevention and Management Plan**

4. Roles and responsibilities

4.1. The **governing board** is responsible for:

- Reviewing this policy on an **annual** basis.

4.2. The **headteacher** is responsible for:

- Ensuring the provisions in this policy are implemented consistently.

4.3. The data protection officer (DPO) is responsible for:

- Monitoring the school'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. Monitoring and review

5.1. The **governing board** will review this policy on an **annual** basis.

5.2. The next scheduled review date for this policy is **February 2023**

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