CUBITT TOWN PRIMARY SCHOOL

# Protection of Biometric Data Policy

*Every child grows • Every voice matters • Every day counts*

This policy applies to pupils, parents and carers, staff and governors

| | |
|---|---|
| **Approved by** | Full Governing Body |
| **Date approved** | |
| **Review date** | |
| **Data Protection Officer** | |

# 1. Our vision and values

At Cubitt Town Primary School, **together we strive for excellence** in an environment that supports both learning and the wellbeing of all. Keeping children safe includes keeping their personal information safe. Our promise that **every voice matters** means that parents, carers and children are always told how their information is used, and have a real say in it. Our 6C values of **Care** and **Commitment** guide how carefully we look after the personal data we hold.

# 2. Our position

**Cubitt Town Primary School does not collect or use biometric data** from pupils or staff, and has no current plans to do so.

If the school ever decides that using biometric data would be helpful, it will follow the law and the Department for Education (DfE) guidance **Protection of biometric information of children in schools and colleges** (updated July 2022), and any later updates, in full. The arrangements that would apply are set out in section 5.

# 3. What is biometric data?

Biometric data is personal information about a person's physical or behavioural characteristics that can be used to identify them – for example, fingerprints, facial shape, retina and iris patterns, voice, and hand measurements.

An **automated biometric recognition system** uses technology to measure these characteristics and compare them with stored information in order to recognise a person – for example, a fingerprint scanner used to pay for school meals or borrow library books, or facial recognition used for entry to a building.

# 4. The law

- **UK GDPR and the Data Protection Act 2018:** biometric data used to identify a person is **special category data**. It must be processed lawfully, fairly and transparently, kept secure, used only for the purpose it was collected for, and not kept for longer than needed. A data protection impact assessment (DPIA) must be completed before any system is introduced.
- **Protection of Freedoms Act 2012 (sections 26 to 28):** before using a pupil's biometric data in an automated recognition system, the school must notify each parent and obtain the **written consent of at least one parent**. The data must not be processed if any parent objects in writing, or if the **pupil objects or refuses** to take part – whatever their age. There are no circumstances in which a school can lawfully process a pupil's biometric data without notifying parents and obtaining the necessary consent.
- Schools must provide a **reasonable alternative** for any pupil whose biometric data is not used, so that they are not disadvantaged.

# 5. If the school introduced a biometric system

Before introducing any system that uses biometric data, the school would:

- discuss the proposal with the Governing Body and the Data Protection Officer, and complete a data protection impact assessment;
- write to every parent and carer, in plain language and, where needed, in home languages, explaining what data would be collected, why, how it would be used and stored, and who it would be shared with;

- obtain written consent from at least one parent before using any pupil's biometric data, and respect any written objection from a parent;
- explain the system to pupils in an age-appropriate way, and respect any pupil's objection or refusal to take part;
- provide an equally convenient alternative (for example, a PIN or card) for anyone who does not take part;
- obtain written consent from any member of staff whose biometric data would be used, and offer them an alternative;
- keep biometric data secure and use it only for the stated purpose;
- delete a person's biometric data when they leave the school, withdraw consent, or object, or when the system is no longer used.

Parents, carers, pupils and staff can withdraw their consent at any time, by contacting the school office or the Data Protection Officer.

## 6. Related policies and review

This policy should be read alongside our Data Protection Policy, Privacy Notices, Online Safety Policy, and Retention and Destruction Policy. It will be reviewed every three years, or sooner if the law or guidance changes or the school considers introducing a biometric system.