

Protection of Biometric Information Policy

Tewkesbury C of E Primary School & Pre-School



Approved by:	Governing Board
Last reviewed on:	February 2026
Next review due by:	February 2027



Where the terms “school” or “organisation” are used throughout this policy, they refer to Tewkesbury C of E Primary School, Tewkesbury C of E Pre-School, and the school’s extended services including Breakfast Club and Afterschool Club.

Contents

1.	Purpose of this policy	Page 3
2.	What is biometric information	Page 3
3.	Current use of biometric systems	Page 3
4.	Legal requirements and consent	Page 3
5.	Notification and information	Page 4
6.	Data protection and security	Page 4
7.	Data Protection Impact Assessments (DPIAs)	Page 4
8.	Roles and responsibilities	Page 4
9.	Complaints	Page 5
10.	Monitoring and review	Page 5
11.	Links to other policies	Page 5

1. Purpose of this policy

This policy sets out how Tewkesbury C of E Primary School protects biometric information and ensures compliance with:

- The Protection of Freedoms Act 2012
- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018

The school recognises that biometric information is particularly sensitive and requires a high level of protection.

2. What is biometric information?

Biometric information is personal data relating to an individual's physical, physiological or behavioural characteristics that can be used to identify them. This includes, but is not limited to:

- Fingerprints
- Facial recognition data
- Retina or iris scans

Under data protection law, biometric data used for identification purposes is classed as special category personal data.

3. Current use of biometric systems

The school does not currently use biometric information for pupils.

Biometric systems may be used for staff access and for authorised groups using **the premises**, for example for building entry and security purposes.

If the school proposes to introduce biometric recognition systems for pupils in the future, this will only take place in line with the requirements set out in this policy.

4. Legal requirements and consent

In accordance with the Protection of Freedoms Act 2012:

- The school will not process a pupil's biometric information without written consent from at least one parent/carers with parental responsibility.
- No pupil will be required to use a biometric system, even where parental consent has been given.
- Pupils will not be disadvantaged in any way if biometric systems are not used.
- A pupil's objection to the use of biometric systems will be respected at all times.

Parents/carers and pupils have the right to:

- Refuse consent for the collection or use of biometric information
- Withdraw consent at any time

If consent is refused or withdrawn, the school will ensure that a suitable alternative arrangement is available.

5. Notification and information

Before any biometric recognition system is introduced for pupils, the school will:

- Inform parents/carers in writing
- Explain how the data will be collected, used, stored and destroyed
- Explain the purpose of the system
- Clearly set out the rights of parents/carers and pupils

6. Data protection and security

The school will ensure that biometric information is:

- Collected lawfully, fairly and transparently
- Used only for the specific purpose for which it was collected
- Stored securely and protected against unauthorised access
- Kept only for as long as necessary
- Permanently destroyed when it is no longer required

Biometric data will not be shared with third parties unless there is a lawful reason to do so.

7. Data Protection Impact Assessments (DPIAs)

Before introducing or significantly changing any biometric system, the school will complete a **Data Protection Impact Assessment (DPIA)** to:

- Identify and minimise privacy risks
- Ensure the system is necessary and proportionate
- Confirm that appropriate safeguards are in place

The school's Data Protection Officer (DPO) will be consulted as part of this process.

8. Roles and responsibilities

Governing Board

The governing board is responsible for ensuring that the school complies with its legal duties in relation to biometric information.

Headteacher

The headteacher is responsible for:

- Ensuring this policy is implemented
- Ensuring consent procedures are followed
- Liaising with the Data Protection Officer

Data Protection Officer (DPO)

The DPO will:

- Advise on compliance with data protection legislation
- Support the completion of DPIAs
- Act as a point of contact for data protection concerns

9. Complaints

Any concerns or complaints relating to the use of biometric information should be raised with the Headteacher in the first instance.

If concerns are not resolved, parents/carers may follow the school's Complaints Policy.

10. Monitoring and review

This policy will be reviewed annually by the governing board, or earlier if there are changes to legislation or the school's use of biometric systems.

11. Links to other policies

This policy should be read alongside:

- Data Protection Policy
- Safeguarding and Child Protection Policy
- Online Safety Policy
- Complaints Policy