WOODLANDS SCHOOL

Protection of Biometric Data Policy

Date policy last reviewed: October 2026

Signed by:

K Haworth	Headteacher	Date:
K Penny	Chair of governors	Date:

Contents:

Statement of intent

1. Legal framework
2. Definitions
3. Roles and responsibilities
4. Data protection principles
5. Data protection impact assessments (DPIAs)
6. Notification and consent
7. Alternative arrangements
8. Storage and data retention
9. Security and breaches
10. Monitoring and review

Appendices

A. Parental notification and consent form for the use of biometric data

Statement of intent

Woodlands School is committed to protecting the personal data of pupils, staff and other individuals, including biometric information. The school will use automated biometric recognition systems only where their use is necessary and proportionate, legally justified, transparent, secure and accessible. No pupil will be disadvantaged for not participating.

1. Legal framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Protection of Freedoms Act 2012
- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR)
- DfE (2026) 'Protection of biometric information of children in schools and colleges'
- DfE (2026) 'Data protection: a guide for schools'
- ICO (2024) 'Biometric Data and the UK GDPR: Updated Guidance'
  DfE (2026) 'Data protection in schools'.
  DfE (2026) 'Keeping Children Safe in Education'

This policy operates in conjunction with the following school policies:

- Data Protection Policy
- Records Management Policy
- privacy notices and Data and Cyber-security Breach Prevention and Management Plan.

2. Definitions

"Biometric data" is personal data resulting from specific technical processing of physical, physiological or behavioural characteristics, such as fingerprints, facial features or voice patterns, which allows or confirms unique identification. Biometric data processed for uniquely identifying a person is special category data under UK GDPR.

An "**automated biometric"** recognition system electronically compares biometric information collected from a person with stored biometric information to recognise or identify them. Processing includes collection, enrolment, storage, comparison, disclosure and deletion, including processing of biometric templates.

"**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.

"**Special category data**" is personal data which the UK GDPR says is more sensitive, and so needs more protection. Where biometric data is used for identification purposes, e.g. through keystroke analysis, it is considered special category data.

3. Roles and responsibilities

- The governing board approves and reviews this policy annually and sooner where law, guidance or systems change.
- The headteacher ensures implementation, staff training, suitable alternative arrangements and compliance with the school's safeguarding and accessibility duties.
- The data controller determines the purpose and means of processing and documents lawful grounds, contracts and retention arrangements.
- The Data Protection Officer (DPO) advises on compliance, oversees the data protection impact assessment (DPIA), monitors arrangements and acts as contact for the ICO and individuals.
- Staff report concerns and suspected incidents promptly under the school's breach procedures and respect all objections.

4. Data protection principles

- The school will process personal data lawfully, fairly and transparently; for specified purposes; only to the extent necessary; accurately; for no longer than necessary; and with appropriate security. The school will demonstrate accountability through its records of processing, DPIA, privacy notices, supplier agreements and review records.
- Before processing begins, the school will identify and document an Article 6 UK GDPR lawful basis and, for special category biometric data, a separate Article 9 condition. Written parental consent under the Protection of Freedoms Act 2012 is an additional requirement for pupils under 18 using automated biometric recognition systems; it is not, by itself, a substitute for the UK GDPR assessment. The DPO will assess whether any consent relied upon under UK GDPR is freely given and valid, particularly in the employment context.

As the data controller, the school is responsible for being able to demonstrate its compliance with the provisions outlined above.

5. Data protection impact assessments (DPIAs)

- Before introducing or materially changing a biometric recognition system, the school will complete and record a DPIA. It will consider the purpose, necessity, proportionality, less intrusive alternatives, pupils' particular needs, risks of exclusion or bias, retention, supplier access, security and mitigation. The DPO will advise and the school will review the DPIA when circumstances change. Where high residual risk cannot be mitigated, the school will consult the ICO before processing.
- Where a supplier processes data on the school's behalf, an appropriate Article 28 UK GDPR contract will set out instructions, access, security, sub-processors, breach notification, return and deletion. International transfers, if any, will be separately assessed.

6. Notification, Consent and the Right to Object

Before taking or using a pupil's biometric information in an automated recognition system, the school will notify each parent, subject to the statutory exceptions, and obtain written consent from

at least one parent or other person entitled to consent under the Protection of Freedoms Act 2012. If a parent objects in writing, or a pupil objects or refuses verbally or non-verbally, the school will not process the pupil's biometric information, regardless of another parent's consent. A pupil's objection does not have to be in writing.

Parents may withdraw consent or object in writing at any time. The school will stop the relevant processing and delete biometric data no longer lawfully required. The school will explain the purpose, data collected, use, storage, retention, sharing, rights, contact details and alternatives in accessible information and its privacy notice.

Woodlands School will recognise communication through speech, gesture, behaviour, symbols, communication aids and other individual methods. Staff will explain the system in ways appropriate to each pupil's age, understanding and communication needs and will respond to indications of refusal. No pupil will be compelled to participate.

Staff and other adults will be informed of the system and their data protection rights. The school will establish a valid lawful basis and special category condition for any adult processing, with genuine alternatives where consent is relied upon.

7. Alternative arrangements

Pupils and adults who do not participate will have a reasonable, accessible and non-stigmatising way to use the same service, without extra cost, delay or disadvantage. The alternative will be suitable for pupils with SEND and will not depend on a pupil being able to handle cash or use a particular communication method.

8. Storage, Retention and Deletion

Biometric data and templates will be stored securely, with access restricted to authorised persons. The school will document what the system actually stores, where it is stored, supplier access and the applicable retention schedule. Data will not be repurposed without a new lawful assessment and appropriate information and permissions.

When a pupil leaves, ceases to use the system, objects or consent is withdrawn, the school will promptly stop processing and securely delete the biometric data from live systems and instruct processors to do the same, subject to any applicable legal requirement. Backup deletion and confirmation will follow documented technical schedules. Consent and audit records will be retained only for their separately documented lawful periods.

9. Security, Incidents and breaches

Security measures will be informed by the DPIA and include proportionate access controls, encryption where appropriate, supplier assurance, system testing, staff training and secure deletion.

All suspected biometric data incidents must be reported to the DPO immediately and in any event within the school's internal 24-hour reporting target.

The school will assess each personal data breach and notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of a breach likely to result in a risk to individuals' rights and freedoms. Where a breach is likely to result in a high risk, affected individuals will be informed without undue delay, subject to applicable exceptions. The school will document breaches, decisions and remedial action.

10. Monitoring and Review

The governing board will review this policy annually, with the next scheduled review proposed for September 2027 following approval of this revision, or sooner following material changes in legislation, guidance, school systems or a significant incident. The DPO will advise on changes and the school will communicate relevant updates to staff, parents and pupils.

1. Appendix A — Parental notification and consent form

This form must be completed for the specific system and checked against the school privacy notice and DPIA before issue.

Dear parent/carer,

Woodlands School proposes to use an automated biometric recognition system for the following service: [INSERT SERVICE AND PURPOSE].

Biometric information collected	**[INSERT TYPE, e.g. fingerprint template]**
How the system works and what is stored	[INSERT VERIFIED DESCRIPTION; do not assume no image is stored]
Purpose and lawful processing information	[INSERT PURPOSE; provide privacy notice and DPO contact]
Supplier and other recipients	[INSERT SUPPLIER, SHARING AND LOCATION DETAILS]
Retention and deletion	[INSERT SPECIFIC RETENTION/DELETION ARRANGEMENTS]
Accessible alternative	[INSERT NON-BIOMETRIC OPTION]
DPO contact	[INSERT CONTACT DETAILS]
Return form by	[INSERT DATE]

Under the Protection of Freedoms Act 2012, the school must notify parents and obtain written consent from at least one parent before processing a child's biometric information in an automated recognition system. Another parent's written objection overrides consent; your child may object or refuse at any time, including non-verbally, regardless of parental consent. You may withdraw consent or object in writing at any time. The school will provide a reasonable alternative without disadvantage.

Please tick one option:

☐ I consent to the use of my child's biometric information for the purpose specified above.

☐ I do not consent to the use of my child's biometric information.

Child's name: _____

Parent/carer's name: _____

Signature: _____ Date: _____

Please return this form to the school office by [INSERT DATE].

2. Appendix B — Reference links and implementation checks

DfE: Protection of children's biometric information in schools (updated 17 June 2026) https://www.gov.uk/government/publications/protection-of-biometric-information-of-children-in-schools

DfE: Data protection in schools (updated 9 July 2026) https://www.gov.uk/guidance/data-protection-in-schools

DfE: Keeping children safe in education 2026 https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

ICO: How do we process biometric data lawfully? https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-process-biometric-data-lawfully/

Before approval: confirm whether Woodlands currently operates a biometric system; confirm the controller, supplier, data stored, lawful grounds, DPIA, privacy notice, retention schedule and accessible alternative. Complete all bracketed fields in Appendix A before issuing it. Record actual approval and signature date.