



# BIOMETRIC POLICY

Silverwood School is committed to promoting equality, inclusion and fairness for all members of our school community. We ensure that all pupils, families and staff are treated with respect and that no individual is disadvantaged through discrimination or unequal access to services.

In developing this policy, the school has carefully considered its responsibilities under the Public Sector Equality Duty (PSED). We have reviewed the potential impact of the policy on individuals with protected characteristics to ensure that it supports our duty to eliminate discrimination, advance equality of opportunity and foster positive relationships within the school community.

Where biometric systems are used within the school, they are implemented in a way that is fair, transparent and accessible for all pupils. Alternative arrangements are always available for pupils who choose not to use biometric identification or where consent is not provided. The school ensures that all processes relating to biometric data are managed responsibly, with appropriate safeguards in place to protect pupils' rights, privacy and wellbeing.

<b>Approved by:</b>	<b>Resource Committee</b>	<b>Date: 18/03/2026</b>
---------------------	---------------------------	-------------------------

<b>Last reviewed on:</b>	<b>March 2026 (ratified by FGB April 2026)</b>
--------------------------	--

<b>Next review by:</b>	<b>March 2027</b>
------------------------	-------------------

## Introduction

Silverwood School is committed to protecting the personal data of all its pupils and staff. This includes biometric data. We collect and process biometric data in accordance with relevant legislation and guidance to ensure the data and the rights of individuals are protected. This policy outlines the procedure the school follows when collecting and processing biometric data and applies to parents and pupils, staff and visitors alike.

## Legal Framework

This policy has due regard to the following legislation and guidance:

- Protection of Freedoms Act 2012
- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR)
- The DfE guidance “Protection of biometric information of children in schools and colleges”

It should be read in conjunction with the following school policies:

- Data Protection Policy
- Records Management and Retention Policy
- Security Breach Prevention and Management Policy

## Definitions

- **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.
- **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.
- **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 students.

- **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.

## Roles and responsibilities

The Governing Body is responsible for reviewing this policy annually.

The Executive Headteacher is responsible for ensuring the provisions in this policy are implemented consistently.

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.
- Being the first point of contact for the ICO and for individuals whose data is processed by the school and connected third parties.

### Data protection principles

The school processes all personal data, including biometric data, in accordance with the key principles set out in the UK GDPR.

The school ensures biometric data is:

- Processed lawfully, fairly and in a transparent manner;
- Only collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
  - Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- Accurate and, where necessary, kept up-to-date. Reasonable steps are taken to ensure inaccurate information is rectified or erased;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed;
- Processed in a manner that ensures appropriate security of the information, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

As the data controller the school is responsible for compliance with the above.

### Notification and Consent

Where the school uses pupils' biometric data as part of an automated biometric recognition system, the school will comply with the requirements of the Protection of Freedoms Act 2012. The consent requirements for biometric information are imposed by section 26 of this Act.

Prior to any biometric recognition system being put in place or to processing a pupils' biometric data, the school will complete a Data Protection Impact Assessment in accordance with the school's Data Protection Policy. The school will then notify pupils' parents/carers how the data will be processed (collected, used, stored and ultimately disposed). The notification will include information regarding the following:

- Details about the type of biometric information to be taken;
- How the data will be used;
- The parent's and the pupils' right to refuse or withdraw their consent;
- The school's duty to provide reasonable alternative arrangements for those pupils whose information cannot be processed.

Written consent will be sought from at least one parent of the pupil before the school collects or uses a pupil's biometric data. Consent for the processing of biometric data will be obtained in accordance with the consent procedures set out in the school's Data Protection Policy. Where parental consent is required, the school will follow its established processes for identifying and contacting parents or carers recorded on the school's admissions register.

Where neither parent of a pupil can be notified for any of the reasons above, consent will be sought from the following individuals or agencies as appropriate:

- If a pupil is being 'looked after' by the LA or is accommodated or maintained by a voluntary organisation, the LA or voluntary organisation will be notified and their written consent obtained;
- If the above does not apply then notification will be sent to all those caring for the pupil and written consent will be obtained from at least one carer before the pupil's biometric data can be processed.

The school will not process the biometric data of a pupil under the age of 18 in the following circumstances:

- The pupil (verbally or non-verbally) objects or refuses to participate in the processing of their biometric data;
- No parent or carer has consented in writing to the processing;
- A parent has objected in writing to such processing, even if another parent has given written consent.

Parents and pupils can object to use of their biometric data and withdraw their consent at any time. Where this happens, any biometric data relating to the pupil that has already been captured will be deleted.

If a pupil does not want their biometric data to be used, the school will ensure that it is not collected or used in the school's biometric systems, even if parental consent has been given. This applies specifically to systems such as fingerprint recognition for meals or door access.

Biometric data collected as part of treatment or therapy, such as voice recordings, will only be used for the purpose for which it was collected and will not be used in the school's biometric systems. This ensures that pupils and parents can be confident that personal data collected for therapy or educational purposes is kept separate and is not repurposed.

Where staff members or other adults use the school's biometric system(s), consent will be obtained from them before they use the system. Staff and visitors can object to taking part in the school's biometric system(s) and can withdraw their consent at any time. Where this happens any biometric data relating to the individual that has already been captured will be deleted.

Alternative arrangements will be provided to any individual that does not consent to take part in the school's biometric system(s).

#### Alternative arrangements

Parents, pupils, staff members and other relevant individuals have the right to choose not to participate in the school's biometric systems. Where an individual objects to the use of biometric identification, the school will provide a reasonable alternative method to enable them to access the relevant service.

For example, where a biometric system is used for school meal payments, pupils who do not wish to use biometric identification will be able to use an alternative method such as a card or fob.

Any alternative arrangements will ensure that the individual is not disadvantaged, experiences no additional difficulty in accessing the service, and that no additional burden is placed on the individual or, where relevant, their parents or carers.

### Data retention

Biometric data will be managed and retained in line with the school's Records Management and Retention Policy. It will be deleted when the pupil leaves the school.

If an individual (or a pupil's parent, where relevant) withdraws their consent for their/their child's biometric data to be processed, it will be erased from the school's system.