# WOODBRIDGE HIGH SCHOOL

# Biometrics Policy

# Contents

# 1. What is Biometric Data?

Biometric data means personal information about an individual's physical or behavioural characteristics that can be used to identify that person; this can include their fingerprints, facial shape, retina and iris patterns, and hand measurements.

The Information Commissioner considers all biometric information to be personal data as defined by the General Data Protection Regulations (GDPR) and Data Protection Act 2018 (DPA); this means that it must be obtained, used and stored in accordance with these requirements (see relevant paragraphs below).

The Protection of Freedoms Act includes provisions which relate to the use of biometric data in schools and colleges when used as part of an automated biometric recognition system. These provisions are in addition to the requirements of the GDPR and DPA. (See relevant section below).

# 2. What is an Automated Biometric Recognition System?

An *automated biometric recognition system* uses technology 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.

Biometric recognition systems can use many kinds of physical or behavioural characteristics such as those listed in 1) above.

# 3. What Does Processing Data Mean?

The term 'Processing' is defined under the GDPR and DPA as any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

An automated biometric recognition system processes data when:

a. recording pupils' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner;

b. storing pupils' biometric information on a database system; or

c. using that data as part of an electronic process, for example, by comparing it with biometric information stored on a database in order to identify or recognise pupils.

# 4. The Protection of Freedoms Act 2012

**Notification and Parental Consent (where the data are to be used as part of an automated Biometric recognition system)** (see 2 above), schools and colleges must also comply with the additional requirements in sections 26 to 28 of the **Protection of Freedoms Act 2012**.)

The written consent of at least one parent must be obtained before the data are taken from the child and used (i.e. **'processed'** – see 3 above). This applies to all pupils in schools and colleges **under the age of 18.** In no circumstances can a child's biometric data be processed without written consent.

*What the law says:*

1) Schools and colleges must notify each parent of a pupil under the age of 18 if they wish to take and subsequently use the child's biometric data as part of an automated biometric recognition system.

2) As long as the child or a parent does not object, the written consent of only one parent will be required for a school or college to process the child's biometric information. A child does not have to object in writing but a parent's objection must be written.

3) Schools and colleges will not need to notify a particular parent or seek his or her consent if the school or college is satisfied that:

a. the parent cannot be found, for example, his or her whereabouts or identity is not known;

b. the parent lacks the mental capacity to object or to consent;

c. the welfare of the child requires that a particular parent is not contacted, for example where a child has been separated from an abusive parent who is not to be informed of the child's whereabouts; or

d. where it is otherwise not reasonably practicable for a particular parent to be notified or for his or her consent to be obtained.

4) Where neither of the parents of a child can be notified for one of the reasons set out above (which would mean consent cannot be obtained from either of them), section 27 of the Protection of Freedoms Act 2012 sets out who should, in such circumstances, be notified and who can give consent:

(a) if the child is being 'looked after' by a local authority or is accommodated or maintained by a voluntary organisation (i.e. a not-for-profit organisation), the local authority, or as the case may be, the voluntary organisation must be notified and their written consent obtained.

(b) if paragraph (a) above does not apply, then notification must be sent to all those caring for the child and written consent must be gained from at least one carer before the child's biometric data can be processed (subject to the child and none of the carers objecting in writing).

There will never be any circumstances in which a school or college can lawfully process a child's biometric information (for the purposes of using an automated biometric recognition system) without one of the persons above having given written consent.

5) Under the Education (Pupil Registration) Regulations 2006, schools are required to keep an admissions register that includes the name and address of every person known to the school to be a parent of the child, including non-resident parents. Schools that wish to notify and seek consent to process a child's biometric information at any point after the enrolment of a child should have contact details for most parents in the admission register.

6) Schools should be alert to the fact that the admission register may, for some reason, not include the details of both parents. Where the name of only one parent is included in the admission register, schools should consider whether any reasonable steps can or should be taken to ascertain the details of the other parent. For example, the school might ask the parent who is included in the admission register or, where the school is aware of local authority or other agency involvement with the child and its family, may make enquiries with the local authority or other agency. Schools and colleges are not expected to engage the services of 'people tracer' or detective agencies but are expected to take reasonable steps to locate a parent before they are able to rely on the exemption in section 27(1)(a) of the Protection of Freedoms Act (i.e. notification of a parent not required if the parent cannot be found).

7) An option would be for schools and colleges to notify parents that they intend to take and use their child's biometric information as part of an automated biometric recognition system and seek written consent to do so at the same time as obtaining details of parents as part of the enrolment process. In other words, details of both parents would be requested by the school or college for both purposes (enrolment and notification of intention to process biometric information).

8) Notification sent to parents should include information about the processing of their child's biometric information that is sufficient to ensure that parents are fully informed about what is being proposed. This should include: details about the type of biometric information to be taken; how it will be used; the parents' and the pupil's right to refuse or withdraw their consent; and the school's duty to provide reasonable alternative arrangements for those pupils whose information cannot be processed. A suggested sample 'Notification and Consent' template is included at the end of this advice.

### The pupil's right to refuse

*What the law says:*

1) If a pupil under 18 objects or refuses to participate (or to continue to participate) in activities that involve the processing of their biometric data, the school or college must ensure that the pupil's biometric data are not taken/used as part of a biometric recognition system. A pupil's objection or refusal overrides any parental consent to the processing.

Schools and colleges should take steps to ensure that pupils understand that they can object or refuse to allow their biometric data to be taken/used and that, if they do this, the school or college will have to provide them with an

alternative method of accessing relevant services. The steps taken by schools and colleges to inform pupils should take account of their age and level of understanding. Parents should also be told of their child's right to object or refuse and be encouraged to discuss this with their child.

3) In addition to the required actions for notification and obtaining consent, schools and colleges may wish to include information in their privacy notices and explain how biometric data is to be processed and stored by the school.

### Providing alternatives

*What the law says:*

1) Reasonable alternative arrangements must be provided for pupils who do not use automated biometric recognition systems either because their parents have refused consent (or a parent has objected in writing) or due to the pupil's own refusal to participate in the collection of their biometric data.

2) The alternative arrangements should ensure that pupils do not suffer any disadvantage or difficulty in accessing services/premises etc. as a result of their not participating in an automated biometric recognition system. Likewise, such arrangements should not place any additional burden on parents whose children are not participating in such a system.

## 5. The General Data Protection Regulations (GDPR) and Data Protection Act 2018 (DPA)

As *data controllers*, schools and colleges must process pupils' *personal data* (which includes biometric data), in accordance with the General Data Protection Regulations (GDPR) and Data Protection Act 2018 (DPA 2018). The provisions in the Protection of Freedoms Act 2012 are in addition to the requirements under the DPA with which schools and colleges must continue to comply.

The GDPR and DPA 2018 have six data protection principles with which all data controllers must comply.

When processing a pupil's personal data, including biometric data for the purposes of an automated biometric recognition system, schools and colleges must comply with these principles. This means, for example, that they are required to:

a. Store biometric data securely to prevent any unauthorised or unlawful use.

b. Not keep biometric data for longer than it is needed meaning that a school or college must destroy a child's biometric data if, for whatever reason, the child no longer uses the system including when he or she leaves the school or college or where a parent withdraws consent or the child objects.

c. Ensure that biometric data is used only for the purposes for which they are obtained and that such data are not unlawfully disclosed to third parties.

### Special Category data

You must still have a lawful basis for your processing under Article 6, in exactly the same way as for any other personal data. The difference is that you will also need to satisfy a specific condition under Article 9.

This is because special category data is more sensitive, and so needs more protection. Biometrics data is considered to be special category data.

Your choice of lawful basis under Article 6 does not dictate which special category condition you must apply, and vice versa. For example, if you use consent as your lawful basis, you are not restricted to using explicit consent for special category processing under Article 9.

# 6. Text of Letter Circulated to Parents/Carers

Dear Parent/Carer,

**Biometric Information System**

We have used a biometric system at Woodbridge for the last six years. It has proved to be very efficient, safe and easy to use for both the canteen and printers. We now use two systems, one for the canteen (iDStore) and one for the printers (Biostore iDManager). Over 96% of the students are registered on our systems with the remainder either opting out or unable to use it. Additional information can be found under 'What is biometrics?' further down the letter.

Woodbridge has complied with the Data Protection Act 1998 with regard to the biometric systems. Legislation (Protection of Freedoms Act 2012) means parents/carers are required to give consent ('opt in') in order for the school to use biometric information. You can opt-out at any time. The alternative method is the use of a PIN number.

Please complete the permission slip below in order for your child to use the biometric systems for the canteen and printers.

Yours sincerely,

Mr J Clifton

Assistant Headteacher

**********

**What is biometrics?**
A scanner takes measurements of your child's fingerprint which is converted into mathematical representations of certain points of the finger image and stored on the school's secure systems. An image of your child's fingerprint is not stored and the original fingerprint cannot be reconstructed.

**********

**Biometric Information Permission Slip** – please tick one of the boxes. Consent can be updated or removed at any time by emailing the school.

☐ **I give permission** for the school to use biometric information from my child as part of the canteen and printer systems.

☐ **I do not give permission** for the school to use biometric information from my child as part of the canteen and printer systems.

Child's name

Child's date of birth .....

Parent/carer name

Parent/carer email address .....

Parent/carer signature .....

Date .....

Approval: Approved by the F&GP Committee on 7th February 2024

Reviewer: Headteacher and School Business & Finance Manager

Date of Next Review: Spring 2025