Protection of biometric information of children in schools

Approved by:	Governing Body	**Date:** May 2025
Last reviewed on:	May 2024	
Next review due by:	May 2026	

General Principles

This policy explains the legal duties Wellington School has if we wish to use biometric information about pupils for the purposes of using automated biometric recognition systems.

Key Points:

• Schools and colleges that use pupils' biometric data (see 1 below) must treat the data collected with appropriate care and must comply with the data protection principles as set out in the Data Protection Act 1998.

• Where the data is used as part of an automated biometric recognition system (see 2 below), schools and colleges must also comply with the additional requirements in sections 26 to 28 of the Protection of Freedoms Act 2012 (see relevant section below)

• Schools and colleges must ensure that each parent of a child is notified of the school's intention to use the child's biometric data (see 1 below) as part of an automated biometric recognition system.

• The written consent of at least one parent/carer/legal guardian must be obtained before the data is taken from the child and used (i.e. 'processed' – see 3 below). 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.

• Schools and colleges must not process the biometric data of a pupil (under 18 years of age) where:

a) the child (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data;

b) no parent/carer/legal guardian has consented in writing to the processing; or

c) a parent/carer/legal guardian has objected in writing to such processing, even if another parent/carer/legal guardian has given
written consent.

• Schools and colleges must provide reasonable alternative means of accessing services for those pupils who will not be using an automated biometric recognition system.

What is biometric data?

1) 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.

2) The Information Commissioner considers all biometric information to be personal

data as defined by the Data Protection Act 1998; this means that it must be obtained, used and stored in accordance with that Act (see relevant paragraphs below).

3) 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 Data Protection Act 1998. (See relevant section below).

What does processing data mean?

'Processing' of biometric information includes obtaining, recording or holding the data or carrying out any operation or set of operations on the data including (but not limited to) disclosing it, deleting it, organising it or altering it.

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.

The Protection of Freedoms Act 2012

Notification and Parental 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/carer/legal guardian or seek his or her consent if the school or college is satisfied that:

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

b. the parent/carer/legal guardian lacks the mental capacity to object or to consent;

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

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

4) Where neither of the parents/carers/legal guardians 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).

5) 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.

6) 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.

7) 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).

8) 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).

9) 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.

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.

Also note:

2) 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.

The Data Protection Act 1998

1) As data controllers, schools and colleges must process pupils' personal data (which includes biometric data), in accordance with the Data Protection Act 1998 (DPA). 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.

2) The DPA has eight data protection principles with which all data controllers must comply.

3) 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.

For further more information about the data protection principles and practical advice, see the Associated Resources section below.

4) New data protection legislation is due to come into force in the UK by 25th May 2018. This legislation will have an impact on how pupils' biometric data should be processed. We strongly recommend that schools and any persons with responsibility for processing pupils' biometric data seek independent legal advice to ensure that they comply with any changes to data protection law.

Associated Resources

DfE guidelines for schools on communicating with parents and obtaining consent: https://www.gov.uk/government/publications/dealing-with-issues-relating-toparental-responsibility.

ICO guide to data protection:
http://www.ico.gov.uk/for_organisations/data_protection/the_guide.aspx.

ICO guidance on data protection for education establishments:
http://www.ico.gov.uk/for_organisations/sector_guides/education.aspx.

British Standards Institute guide to biometrics: Biometrics Website for news updates standards - biometric systems - BSI Shop.