

# Protection of Biometric Information of children in Schools



## All Hallows Catholic School

### Document Control

Date	Version	Changes	Senior Leadership Team Approval	Governing Body Approval
6 May 21	V1.0	Updated into new format	C Antrobus	I Anderson
14 May 21	V1.0	Approved & Published	C Antrobus	I Anderson
20 Sept 22	V1.1	Updated for 2022/2023, Approved & Published	C Antrobus	I Anderson

### Review Schedule:

Document Reference [PPL.018](#)

Review Cadence: [Annually](#)

Next review date: [Sept 2023](#)

### Our School Vision

Our vision at All Hallows is to form happy, successful students who reach their full potential and leave the School with integrity and moral purpose. We want a whole School experience that everyone would wish for their own children. We put our students at the heart of everything we do, guided by the truth and love of Christ.

## **1. About this advice**

This is non-statutory guidance from the Department for Education (the department). It explains the legal duties schools and colleges have if they wish to process pupils' and students' individual data using automated biometric technologies that allow for unique identification.

The advice should be read alongside:

The Data Protection Act 2018

The UK General Data Protection Regulation (UK GDPR)

The Protection of Freedoms Act 2012

**This guidance is for:**

- Governing bodies of maintained schools (including maintained nursery schools) and colleges<sup>1</sup>
- Proprietors of independent schools (including academies, free schools and alternative provision academies) and non-maintained special schools. In the case of academies, free schools and alternative provision academies, the proprietor will be the academy trust
- Management committees of pupil referral units (PRUs) senior leadership teams
- Any person(s) responsible for the controlling and/or processing of data within the school or college setting

This guidance replaces any previous advice.

<sup>1</sup>including FE college corporations, sixth-form college corporations and bodies conducting designated institutions<sup>2</sup> [Data Protection Act 2018 \(legislation.gov.uk\)](https://www.legislation.gov.uk)

**What legislation does this advice relate to?**

UK GDPR and Protection of Freedoms Act 2012

The Data Protection Act 2018

**Who is this advice for?**

This advice is aimed at proprietors, Governing Bodies, Headteachers and Principals at all schools<sup>1</sup>, sixth form colleges, 16-19 Academies, and further education institutions<sup>2</sup>. However, it should be noted that in all settings it is only students who are under 18 who are still regarded as children and who are therefore subject to the provisions set out in the Protection of Freedoms Act 2012.

It will also be of use to school staff, parents and pupils.

<sup>1</sup> This includes Academies, Free Schools, other types of independent schools, maintained schools and non-maintained special schools

<sup>2</sup> It should be noted further education institutions in this context means (a) institutions conducted by further education corporations; (b) institutions designated under s28 Further and Higher Education Act 1992 ("FHEA"); and (c) sixth form colleges (see s26 and s28 Protection of Freedoms Act 2012 and s91(3) FHEA). Therefore, strictly speaking sixth form colleges are classified as further education institutions, but for clarity have been specified separately in the above paragraph

## **2. Key Points**

- School 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), school must also comply with the additional requirements in sections 26 to 28 of the Protection of Freedoms Act 2012 (see relevant section below).
- School 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 consent of at least one parent 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 school under the age of 18. In no circumstances can a child's biometric data be processed without consent.
- School 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 has consented to the processing; or
  - c) a parent has objected in writing to such processing, even if another parent has given consent.
- School 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 school 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 is an automated biometric recognition system?

1. An automated biometric recognition system uses technology which measures an individual's physical or behavioural characteristics<sup>3</sup> 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.
2. Biometric recognition systems can use many kinds of physical or behavioural characteristics such as those listed in section 1 of the 'What is biometric data' section above.

### 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<sup>4</sup>. An automated biometric recognition system processes data when:

1. a) recording pupils' biometric data, eg, taking measurements from a fingerprint via a 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.
2. More information on these topics is available via the Associated Resources section below.

<sup>3</sup> Biometric systems usually store measurements taken from a person's physical/behavioural characteristics and not images of the characteristics themselves. For example, a fingerprint image is not stored on the system but measurements from the fingerprint are converted into a template and the template is stored. The templates are also biometric data.

<sup>4</sup> See section 1(1) of the Data Protection Act 1998

## 3. About The Protection of Freedoms Act 2012

### Notification and Parental Consent

*What the law says:*

1. School must notify each parent<sup>5</sup> 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 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. School will not need to notify a particular parent or seek their consent if the school is satisfied that:
  - a) the parent cannot be found, for example, their whereabouts or identity is not known;
  - b) the parent lacks the mental capacity<sup>6</sup> 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 their 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<sup>7</sup> 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).

<sup>5</sup> The parents of a child include not only the biological mother or father (or the adoptive parents) but any other individual with parental responsibility for the child. Part 1 of the Children Act 1989 sets out who has parental responsibility and what this means.

<sup>6</sup> Within the meaning of the Mental Capacity Act 2005.

<sup>7</sup> For example, the child is subject to a care order in favour of the local authority or the local authority provides accommodation for the child – see section 22 of the Children Act 1989 for the definition of 'looked after' child.

5. There will never be any circumstances in which a school 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 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 school 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 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. 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 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. School 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 will have to provide them with an alternative method of accessing relevant services. The steps taken by school 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, school may wish to include information in their privacy notices and explain how biometric data is to be processed and stored by the school. Further advice and suggested templates for privacy notices is available for 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 2018

1. As *data controllers*, school must process pupils' *personal data* (which includes biometric data), in accordance with the Data Protection Act 2018 (DPA). The provisions in the Protection of Freedoms Act 2012 are in addition to the requirements under the DPA with which school 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, school 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 must destroy a child's biometric data if, for whatever reason, the child no longer uses the system including when they leave the school 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.

## Associated Resources

- DfE guidelines for schools on communicating with parents and obtaining consent:  
<https://www.gov.uk/government/publications/dealing-with-issues-relating-to-parental-responsibility>.
- ICO guide to data protection:  
[http://www.ico.gov.uk/for\\_organisations/data\\_protection/the\\_guide.aspx](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](http://www.ico.gov.uk/for_organisations/sector_guides/education.aspx).



- British Standards Institute guide to biometrics:  
<https://shop.bsigroup.com/en/Browse-by-Subject/Biometrics/?t=r>

#### **4. Template Notification & Consent Form**

The following is suggested text for a notification letter and consent form for schools to use to notify parents of their plans to collect and use biometric data. Schools may wish to adapt this text in light of their own particular systems but should ensure that parents are made aware of the school's requirements as set out in sections 26-28 of the Protection of Freedoms Act 2012.

#### **NOTIFICATION OF INTENTION TO PROCESS PUPILS' BIOMETRIC INFORMATION**

Dear [name of parent/carer]

The school wishes to use information about your child as part of an automated (i.e. electronically-operated) recognition system. This is for the purposes of [specify what purpose is - e.g. catering, library access]. The information from your child that we wish to use is referred to as 'biometric information' (see next paragraph). Under the Protection of Freedoms Act 2012 (sections 26 to 28), we are required to notify each parent of a child and obtain the written consent of at least one parent before being able to use a child's biometric information for an automated system.

#### **Biometric information and how it will be used**

*Biometric information* is information about a person's physical or behavioural characteristics that can be used to identify them, for example, information from their fingerprint / iris / palm. The school would like to take and use information from your child's fingerprint and use this information for the purpose of providing your child with the ability to purchase goods from the school canteen.

The information will be used as part of an automated biometric recognition system. This system will take measurements of your child's fingerprint and convert these measurements into a template to be stored on the system. An image of your child's fingerprint is not stored. The template (i.e. measurements taken from your child's fingerprint) is what will be used to permit your child to access services.

You should note that the law places specific requirements on school when using personal information, such as biometric information, about pupils for the purposes of an automated biometric recognition system.

For example:

- a) the school cannot use the information for any purpose other than those for which it was originally obtained and made known to the parent(s) (i.e. as stated above);
- b) the school must ensure that the information is stored securely;
- c) the school must tell you what it intends to do with the information;
- d) unless the law allows it, the school cannot disclose personal information to another person/body – you should note that the only person/body that the school wishes to share the information with is the supplier of biometric systems, in order to provide support for the purchasing software in the school canteen.

#### **Providing your consent/objection**

As stated above, in order to be able to use your child's biometric information, the consent of at least one parent is required. However, consent given by one parent will be overridden if the other parent objects in writing to the use of their child's biometric information. Similarly, if your child objects to this, the school cannot collect or use their biometric information for inclusion on the automated recognition system.

You can also object to the proposed processing of your child's biometric information at a later stage or withdraw any consent you have previously given. This means that, if you give consent but later change

your mind, you can withdraw this consent. Please note that any consent, withdrawal of consent or objection from a parent must be in writing.

Even if you have consented, your child can object or refuse at any time to their biometric information being taken/used. Their objection does not need to be in writing. We would appreciate it if you could discuss this with your child and explain to them that they can object to this if they wish.

The school is also happy to answer any questions you or your child may have.

If you do not wish your child's biometric information to be processed by the school, or your child objects to such processing, the law says that we must provide reasonable alternative arrangements for children who are not going to use the biometric system to purchase goods from the school canteen.

Please note that when your child leaves the school, or if for some other reason they ceases to use the biometric system, their biometric data will be securely deleted.

### Further information and guidance

This can be found via the following links:

Department for Education's '*Protection of Biometric Information of Children in Schools – Advice for proprietors, Governing Bodies, Headteachers, principals and school staff*'.

<http://www.education.gov.uk/schools/adminandfinance/schooladmin>.

ICO guide to data protection for organisations:

<https://ico.org.uk/for-organisations/guide-to-data-protection/>

ICO guidance on data protection for education establishments:

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/education-data/>

### CONSENT FOR THE USE OF BIOMETRIC INFORMATION IN SCHOOL

When you accept a place at All Hallows, you will be asked to complete an online form to provide consent to the taking and using of information from your child's biometric fingerprint by All Hallows Catholic School as part of an automated biometric recognition system. This biometric information will be solely used by All Hallows Catholic School for the purpose of purchasing goods from the school canteen.

In completing the online form, you are authorising the school to use your child's biometric information for this purpose until they either leave the school or ceases to use the system. If you wish to withdraw your consent at any time, this must be done so in writing and sent to the school at the following address:

All Hallows Catholic School  
Weybourne Road  
Farnham  
Surrey  
GU9 9HF

Once your child ceases to use the biometric recognition system, their biometric information will be securely deleted by the school.

