Protection of Biometric Data of Children in School Policy

The John Harrox Primary School

Approved by:	Governing Body	**Date:** [18/09/2023]
Last reviewed on:	[18/09/2023]	
Next review due by:	September 2024	

Contents

- Introduction
- This guidance is for
- Review Date
- Overview of the legislation framework
- What this means for schools and colleges
- Biometric Data
- What is Biometric Data?
- What is an Automated Biometric Recognition System?
- What is Facial recognition?
- What is live facial recognition?
- What does processing data mean?
- Data Controller Responsibilities
- The Data Protection Impact Assessment (DPIA)
- Consent
- Who can give consent?
- Pupils' and students' right to refuse
- Privacy Notice
- Provision of Alternative Arrangements
- Management of Information
- Purpose
- Security
- Protections against unlawful and unauthorised access
- Regulatory Functions
- Information Commissioner's Office
- Annex A Protection of Freedoms Act 2012 and Consent
- Annex B Parental Notification Form
- Template Notification Form
- Annex C - Consent to school or college using under 18 biometric data

Introduction

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

NB: The John Harrox Primary School does not currently use automated biometric technologies that allow for unique identification of its pupils.

This guidance is for

- governing bodies of maintained schools (including maintained nursery schools) and colleges
- 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.

Review Date

This guidance will be reviewed annually

Overview of the legislation framework

The Data Protection Act 2018 and the UK GDPR has updated data protection laws for the digital age, in which an ever-increasing amount of personal data is being held and processed.

The Data Protection Act 2018, UK GDPR, and the Protection of Freedoms Act 2012 set out how pupils' and students' data (including biometric data) should be processed. Biometric data is special category data and must be processed lawfully, fairly and in a transparent way. Schools and colleges should ensure that biometric information is kept safe.

Data controllers determine the purpose or outcome of the processing of the personal data. For the purpose of this guidance, schools and colleges are considered to be Data controllers. Data controllers must comply with and demonstrate compliance with all the data protection principles as well as the other UK GDPR requirements. They are also responsible for the compliance of their processor(s).

Data processors act on behalf of and follow the instructions from the controller regarding the processing of personal data.

UK GDPR requires all data controllers and processors to be open and transparent about how and why personal data is used. Data should be processed in line with the following seven UK GDPR principles:

- **lawfulness, fairness and transparency** - Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
- **purpose limitation** - Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- **data minimisation** - Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- **accuracy** - Personal data shall be accurate and, where necessary, kept up to date
- **storage limitation** - Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
- **integrity and confidentiality** - Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
- **accountability** - The controller shall be responsible for and be able to demonstrate compliance with the UK GDPR

This guidance sets out the main points schools and colleges should consider before introducing and when using automated biometric technology. Schools and colleges should ensure that they store and process all personal data within the parameters set out in law, and if using automated biometric technology, meet the requirements set out in:

- **Article 6** of the UK GDPR which sets out the six lawful bases for processing data
- **Article 9** of the UK GDPR which sets out the list of special categories of data and conditions for processing

Biometric data is special category data (Article 9 of the UK GDPR) and can only be processed when the data processor has identified both the lawful basis under Article 6 of the UK GDPR and a separate condition for processing under Article 9 of the UK GDPR. There are also further conditions that may have to be satisfied under Schedule 1 of the Data Protection Act 2018.

If you are uncertain about any aspect of data protection law or the use of automated biometric technology, you should seek independent advice to make sure that you comply with all necessary legislation.

The Information Commissioner's Office (ICO) https://ico.org.uk/ can also provide advice and support on these issues.

The Protection of Freedoms Act 2012 imposes a requirement on schools and colleges to obtain consent from parents of children under 18 years of age before processing the child's biometric information.

What this means for schools and colleges

The decision to use automated biometric technology rests with individual schools and colleges. However, careful consideration should be given to the purpose for use, whether the processing is necessary and proportionate including the implications of using this technology for example, any operational requirements, the use of personal information and possible data breaches as well as the legal requirements associated with the management of it.

The data controller, must ensure that the processing of any biometric data, including any processing carried out by a third party on their behalf complies with the Data Protection Act 2018, UK GDPR and Protection of Freedoms Act 2012.

Biometric Data

What is Biometric Data?

Biometric data means personal information resulting from specific technical processing relating to the individual's physical, psychological or behavioural characteristics which allow or confirm the unique identification of that person, such as facial images, voice recognition or fingerprints.

What is an Automated Biometric Recognition System?

An automated biometric recognition system uses technology to measure an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (i.e. electronically). Biometric systems usually store measurements taken from a person's physical/behavioural characteristics and not images of the characteristics themselves.

What is Facial recognition?

Facial recognition is the process by which a person can be identified or otherwise recognised from a digital facial image. Cameras are used to capture these images and facial recognition technology software produces a biometric template. Often, the system will then estimate the degree of similarity between two facial templates to identify a match (e.g. to verify someone's identity), or to place a template in a particular category (e.g. age group). This type of technology can be used in a variety of contexts from unlocking our mobile phones, to setting up a bank account online, or passing through passport control.

Facial recognition will often not be appropriate in schools and colleges if other options are available to achieve similar goals, like paying for school lunches. Schools and colleges must establish that facial recognition is both necessary and proportionate within the school and college environment.

What is live facial recognition?

Live facial recognition is different to the facial recognition technology referenced above and is typically deployed in a similar way to traditional CCTV. It is directed towards everyone in a particular area rather than specific individuals. It has the ability to capture the biometric data of all individuals passing within range of the camera automatically and indiscriminately. Their data is collected in real-time and potentially on a mass scale.

Live facial recognition is not appropriate in schools or colleges. It would be difficult for a school or college to demonstrate that the use of live facial recognition technology is justified

as fair, necessary, proportionate or lawful under Article 6 and Article 9 of the UK GDPR. There is a separate legal regime in the Data Protection Act 2018 which governs the use of biometric data for law enforcement purposes.

What does processing data mean?

'Processing' of biometric data 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:

- recording pupil/students' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner
- storing pupil/students' biometric information on a database system
- 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 pupil/students'

Data Controller Responsibilities

It is the responsibility of the data controller to identify the additional risks associated with using automated biometric technology by conducting a DPIA ensuring decisions are documented. Controllers should also, be aware of the wider duties placed on them, for example under the Human Rights Act 1998 and Public Sector Equality Act Duty using automated biometric technology. Controllers should also consult with the ICO when making these decisions.

The Data Protection Impact Assessment

Article 35 of the UK GDPR introduces a legal requirement to undertake a DPIA for any high-risk processing.

A DPIA is designed to describe the data processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them.

DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the UK GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the regulations.

DPIAs should not be viewed as a one-off exercise. A DPIA is a 'living' document and process to help you manage and review the risks of the processing and the measures you have put in place on an ongoing basis. You will need to review your DPIA annually or when there are any changes.

As per Article 36 of the UK GDPR, you must consult with the ICO if your DPIA identifies a high risk and you cannot put in place measures to reduce it, in these instances you cannot begin processing until you have consulted with the ICO. Data protection impact assessments | ICO. Further guidance about children and data protection can also be found here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-uk-gdpr/.

Consent

Who can consent?

In order to comply with the requirements of the Protection of Freedoms Act 2012, schools and colleges must notify each parent, carer/legal guardian of the child of their intention to process the child's biometric information, and that the parent may object at any time to the processing of the information. It is important to understand that a child's biometric information must not be processed unless at least one parent of the child consents, and no parent of the child has withdrawn his or her consent, or otherwise objected, to the information being processed. In addition, a pupil's or student's objection or refusal, overrides any parental consent to the processing, therefore any biometric data must not be processed.

The Protection of Freedoms Act 2012 defines a parent to mean "a parent of the child and any individual who is not a parent of the child but who has parental responsibility for the child". Practically it would be person(s) with parental responsibility for the child, be it birth, adoptive or an appointed body, who a school or college would notify and seek consent from to process personal biometric data. Any one parent could give or withhold consent.

Where a child is looked after and is subject to a care order in favour of the local authority or the local authority provides accommodation for the child within the definition of section 22(1) of the Children Act 1989, a school or college would not be required to notify or seek consent from birth parents

Further information can be found at Annex A.

Pupils' and students' right to refuse

If a pupil or student 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/student's biometric data is not taken/used as part of a biometric recognition system. A pupil's or student's objection or refusal overrides any parental consent to the processing. Section 26 and Section 27 of the Protection of Freedoms Act 2012 makes no reference to a lower age limit in terms of a child's right to refuse to participate in sharing their biometric data.

Schools and colleges should also take steps to ensure that pupils and students 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 must provide them with an alternative method of accessing relevant services. The steps taken by schools and colleges to inform pupils and students 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.

Once a student is 18 years old they will be considered an adult and as such parental consent is no longer relevant.

Privacy Notice

In addition to the required actions for notification and obtaining consent, schools and colleges should include information in their privacy notices and explain how biometric data is to be processed and stored by the school or college, including the rights available to individuals in respect of the processing. Further advice and suggested templates for privacy notices is available for schools and colleges at: https://www.gov.uk/government/publications/data-protection-and-privacy-privacy-notices.

Provision of Alternative Arrangements

Reasonable alternative arrangements must be provided for pupils and students 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 or student's own refusal to participate in the collection of their biometric data.

The alternative arrangements should ensure that pupils and students 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.

Management of Information

Purpose

In line with the purpose limitation principle under Data Protection law, schools and colleges can only store and use the biometric information for the purpose for which it was originally obtained and parental/child consent given.

Security

We would expect schools and colleges to carry out the following when considering security of biometric data:

- store biometric data securely to prevent any unauthorised or unlawful use
- not keep biometric data for longer than it is needed meaning that a school or college should destroy a pupil's/student's biometric data if, for whatever reason, they no longer use the system including when leaving the school or college, where a parent withdraws consent or the pupil/student either objects or withdraws consent
- 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

Protections against unlawful and unauthorised access

It is important that schools and colleges understand their responsibilities, when protecting data. Schools and colleges should:

- identify risks that emerge from the initial assessment
- assess what can be done to eliminate or reduce areas of medium/high risk and setaction plans to do so
- consider access controls
- use DPIAs as a part of their risk identification and mitigation procedures ensuringthat the specifics of any flows of personal data between people, systems,organisations and countries have been clearly explained and presented. This willinclude third party providers of any technology used

Regulatory Functions

Information Commissioner's Office

The ICO is the UK's independent body set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

To meet the UK GDPR all organisations handling personal data, including schools and colleges, need to have the right governance measures in place.

Schools and colleges are data controllers in their own right and therefore should ensure they have appropriate registration with the ICO. For more information about registering with the ICO, visit their website: Registration FAQs | ICO

Annex A Protection of Freedoms Act 2012 and Consent

Notification and Parental Consent:

Schools and colleges must notify each parent[1] of a pupil or student 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.

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.

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:

- the parent cannot be found, for example, his or her whereabouts or identity is not known
- the parent lacks the mental capacity[2] to object or to consent
- 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
- where it is otherwise not reasonably practicable for a particular parent to be notified or for his or her consent to be obtained

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:
if the child is being 'looked after' by a local authority3 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
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).

We do not foresee 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.

Under the Education (Pupil Registration) Regulations 2006, schools are required to keep an admission 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. This can be used by schools that wish to notify and seek consent to process a child's biometric information at any point after the enrolment of a child.

---

[1] 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.
[2] Within the meaning of the Mental Capacity Act 2005.

[3] 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.

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 must take reasonable steps 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 2012 (i.e. notification of a parent not required if the parent cannot be found).

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).

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 or student's right to refuse or withdraw their consent; and the school's or college's duty to provide reasonable alternative arrangements for those pupils whose information cannot be processed. Suggested sample 'Notification and Consent' templates are included in Annexes B and C.

Annex B Parental Notification Form

Template Notification Form

The following is suggested text for a notification letter and consent form for schools and colleges to use to notify parents of their plans to collect and use biometric data.

Schools and colleges 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 and college's requirements as set out in sections 26-28 of the Protection of Freedoms Act 2012 in addition to providing privacy information under UK GDPR as set out earlier in the guidance.

NOTIFICATION OF INTENTION TO PROCESS PUPILS' BIOMETRIC INFORMATION

Dear [name of parent/carer]

The school/college 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/college would like to take and use information from your child's [insert biometric to be used] and use this information for the purpose of providing your child with [specify what purpose is].

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

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

For example:

- the school/college cannot use the information for any purpose other than those forwhich it was originally obtained and made known to the parent (s) (i.e. as statedabove)
- the school/college must ensure that the information is stored securely
- the school/college must tell you what it intends to do with the information
- unless the law allows it, the school/college cannot disclose personal information toanother person/body – you should note that the only person/body that theschool/college wishes to share the information with is [insert any third party withwhich the information is to be shared e.g. X supplier of biometric systems]. This isnecessary in order to [say why it needs to be disclosed to the third party]

Providing your consent/objecting

As stated in the guidance, in order to be able to use your child's biometric information, the written 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/college must not 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. [Your child's] 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/college 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/college, 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 automated system to [insert relevant service e.g. access school library].

If you give consent to the processing of your child's biometric information, please sign, date and return the enclosed consent form to the school/college. Please note that when your child leaves the school/college, or if for some other reason he/she ceases to use the biometric system, his/her biometric data will be securely deleted.

Yours sincerely

Annex C - Consent to school or college using under 18 biometric data

CONSENT FORM FOR THE USE OF BIOMETRIC INFORMATION IN SCHOOL/COLLEGE

Please complete this form if you consent to the school/college taking [and using information from your child's [insert biometric – e.g. fingerprint] by [name of school/college] as part of an automated biometric recognition system. This biometric information will be used by [name of school/college] for the purpose of [describe purpose(s) for which this data will be used, e.g. administration of school/college library/canteen].

In signing this form, you are authorising the school/college to use your child's biometric information for this purpose until he/she either leaves the school/college 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/college at the following address:
[insert address]

Once your child ceases to use the biometric recognition system, his/her biometric information will be securely deleted by the school/college.

Having read guidance provided to me by [name of school/college], I give consent to information from the [insert biometric – e.g. fingerprint] of my child:
[insert name of child]
being taken and used by [name of school/college] for use as part of an automated biometric recognition system for [describe purpose(s) for which this data will be used, e.g. administration of school/college library/canteen].

I understand that I can withdraw this consent at any time in writing.

Name of Parent:	
Signature:	
Date:	

Please return this form to: [insert suitable delivery point and name of school/college].