Department for Education

Protection of biometric data of children in schools and colleges

June 2026

Contents

Introduction

This non-statutory guidance from the Department for Education (the department) explains the legal duties schools and colleges have if they wish to process pupils' and students' individual biometric data in biometric recognition systems to uniquely identify them.

Biometric data is data about a person's unique biological or behavioural traits used to identify them.

Examples include:

- fingerprints
- facial recognition data
- iris or retina scans
- DNA

Biometric technologies - such as fingerprint scanning and facial recognition - are increasingly used in schools and colleges to manage activities like cashless catering, library access, and attendance monitoring. These systems process biometric data, which is a form of personal data derived from an individual's physical or behavioural characteristics and used to uniquely identify them. How we process biometric data lawfully, from the Information Commissioner's Office, has more information.

Biometric data can reveal sensitive information and carries high privacy risks, its use in educational settings is therefore subject to strict legal and regulatory controls. In England, schools must comply with a combination of legislation and guidance, primarily:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Protection of Freedoms Act 2012 (specific to children in schools)

Together, these frameworks ensure that biometric data is processed lawfully, fairly, and transparently, with particular emphasis on protecting children, who are considered more vulnerable data subjects.

Who this publication is for

This guidance is for:

- governing bodies of maintained schools (including maintained nursery schools) and colleges[1]
- 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 alternativw provision academies, the proprietor will be the academy trust
- management committees of pupil referral units (PRUs)
- senior leadership teams
- any persons responsible for the controlling or processing of data within the school or college setting

To be referred to as ‘settings’ within this document.

This guidance replaces any previous advice.

Review date

This guidance will be reviewed annually.

[1] This includes further education colleges, sixth-form college corporations and bodies conducting designated institutions.

Overview of the legislation framework

The Data Protection Act 2018, the UK GDPR and the Data (use and access) Act 2025 has updated data protection laws for the digital age.

The Data Protection Act 2018, UK GDPR, and the Protection of Freedoms Act 2012 set out how personal data (including biometric data) should be processed. Biometric data is special category data. When it is used within systems to identify individuals, it must be processed lawfully, fairly and in a transparent ways. Settings should ensure that biometric information is kept safe, as it reflects distinctive features of a person's physical identity that are not easily changed.

Data controllers determine the purpose or outcome of the processing of the personal data. For this guidance, settings are Data controllers. Data controllers must comply with all the data protection principles as well as the other UK GDPR requirements. They are also responsible for the compliance of their processors.

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 7 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 accieental loss, destruction or damage, using appropriate technical or organisation 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 settings should consider before introducing and when using automated biometric technology. They 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 6 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, when used to identify individuals, is special category data (Article 9(1) UK GDPR) and can only be processed when both a lawful basis under Article 6 UK GDPR and a separate condition for processing under Article 9 UK GDPR has been identified. There are 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 biometric recognition systems, you should speak to your data protection officer or check the Data protection in schools guidance on GOV.UK to ensure that you comply with all necessary legislation.

The Information Commissioner's Office (ICO) provides advice and support on these issues. This includes updated detailed guidance on the use of biometric data.

The Protection of Freedoms Act 2012 imposes a requirement on settings to obtain consent from parents of children under 18 years of age before processing the child's biometric information (see further information on page 11).

What this means for settings

The decision to use biometric data in biometric recognition systems rests with individual schools and colleges. Careful consideration should be given to:

- the purpose for use
- whether the processing is necessary and proportionate, including the implications of using this technology, such as 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 is a type of personal information; not all biometric data is automatically considered special category data. Under UK GDPR, biometric data is only classified as special category data when it is used specifically for the purpose of uniquely identifying someone.

This means if you are using biometric personal data that relates to the way someone behaves, looks (or can be otherwise identified) their fingerprints, or their face, or sounds, for example, a person's voice, and you are using specific technologies in order to uniquely identify or recognise the person it relates to, then you are using special category biometric data.

If biometric data is processed without being used to uniquely identify someone then it is considered ordinary personal data.

For the purposes of this guidance, where the term biometric data is used going forward, it refers to special category biometric data.

What is a Biometric Recognition System?

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

It should be noted that biometric recognitions systems do not solely use biometric data, as often by default additional information, such as names and pupil characteristics, are contained within them.

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 2 facial templates to identify a match (for example, to verify someone's identity), or to place a template in a particular category (such as 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 settings for activities such as paying for school lunches, as other more proportionate options are available to achieve similar goals. Settings must establish that facial recognition is both necessary and proportionate within the setting's 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 can 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 settings. 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
- altering it

A biometric recognition system processes data when:

- recording pupils' or students' biometric data – for example, taking measurements from a fingerprint via a fingerprint scanner
- storing pupils' or students' biometric information on a database
- using that data as part of an electronic process – for example, by comparing it with biometric information stored on a database to indeityf or recognise pupils or students

Data controller responsibilities

It is the responsibility of the data controller to identify the risks associated with using biometric recognition technology by conducting a Data Protection Impact Assessment (DPIA), ensuring the decisions are documented. Data 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.

Data Protection Impact Assessment

Article 35 of the UK GDPR introduces a legal requirement to undertake a Data Protection Impact Assessment (DPIA) for any high-risk processing. The ICO has guidance on when a DPIA is required and an example DPIA template.

A DPIA is designed to describe the data processing, assess its necessity and proportionality and help understand and mitigate 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 demonstrate that appropriate measures have been taken to ensure compliance with the legislation.

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 mitigations 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 unmitigated risk. In these instances, you cannot begin processing until you have consulted with the ICO. Data protection impact assessments, from the ICO, has more information. Children and the UK GDPR, also from the ICO, has further guidance about children and data protection.

Consent

Who can give consent?

To comply with the requirements of the Protection of Freedoms Act 2012, schools and colleges must notify each parent, carer or 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 their 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, meaning 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, the local authority can provide consent as the corporate parent, meaning 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's or student's biometric data is not taken or 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.

Settings 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 or 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 settings 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, settings should include information in their privacy notices and explain how biometric data is to be processed and stored by the setting, including the rights available to individuals in respect of the processing. Data protection: privacy notice model documents includes further advice and suggested templates for privacy notices for schools and colleges.

Provision of Alternative Arrangements

Reasonable alternative arrangements must be provided for pupils and students where consent is not give to use biometric recognition systems.

The alternative arrangements should ensure that pupils and students do not suffer any disadvantage or difficulty in accessing services/premises etc. because they are not participating in a 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

As referenced earlier, it is unlikely that biometric recognition systems used will contain only biometric information.

Purpose

In line with the purpose limitation principle under Data Protection law, settings can only store and use the biometric information for the purpose for which it was originally obtained and parental/child consent given. Data protection in schools – Record keeping and management has further information.

Security

Settings should carry out the following when considerting security of biometric data:

- have secure storage for biometric to prevent any unauthorised or unlawful use
- ensure biometric data is not kept for longer than needed. This means that a setting should destroy a pupil's or student's biometric data if, for whatever reason, they no longer use the system. For example when the pupil or student leaves the setting,

where a parent withdraws consent or the pupil or 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 settings understand their responsibilities when protecting data. Settings should:

- use DPIAs as a part of their risk identification and mitigation procedures, ensuring that the specifics of any flows of personal data between people, systems, organisations and countries have been clearly explained and presented. This will include third-party providers of any technology used
- identify risks that emerge from the DPIA
- assess what can be done to mitigate areas of medium/high risk and set action plans to do so
- consider access controls

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.

Settings are data controllers in their own right and should therefore ensure they have appropriate registration with the ICO. Registrations FAQs, from the ICO, has more information.

Annex A - Protection of Freedoms Act 2012 and consent

Notification and parental consent

Settings must notify each parent[2] 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 a 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 setting to process the child's biometric information. A child does not have to object in writing, but a parent's objection must be written.

Settings will not need to notify a particular parent or seek their consent if the school or college is satisfied that:

- the parent cannot be found, for example, their whereabouts or identity is not known
- the parent lacks the mental capacity[3] 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 their 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:

(a) if the child is being 'looked after' by a local authority[4] 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) 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

---

[2] 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.

[3] Within the meaning of the Mental Capacity Act 2005.

[4] 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.

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 a 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.

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 expected to take reasonable steps to locate a parent before they can rely on the exemption in section 27(1)(a) of the Protection of Freedoms Act 2012 (for example, notification of a parent not required if the parent cannot be found).

An option would be for settings 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
- the setting'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 settings to use to notify parents of their plans to collect and use biometric data. Settings may wish to adapt this text considering their own systems but should ensure that parents are made aware of the school's and college's requirements as set out in sections 26 to 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 or carer]

The school/college wishes to use information about your child as part of what is known as a biometric 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 within a biometric recognition 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 a 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 settings when using personal information, such as biometric information, about pupils for the purposes of an automated biometric recognition system.

For example:

- the school or college 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)
- the school or college must ensure that the information is stored securely
- the school or college must tell you what it intends to do with the information
- unless the law allows it, the school/college cannot disclose personal information to another person/body – you should note that the only person/body that the school/college wishes to share the information with is [insert any third party with which the information is to be shared e.g. X supplier of biometric systems]. This is necessary to [say why it needs to be disclosed to the third party]

Providing your consent or objecting

As stated in the guidance, 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.

Annex C – consent to school or college using under 18 biometric data

Consent forms for the use of biometric information in school or 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 a 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].

Department for Education

About this publication:

enquiries www.gov.uk/contact-dfe
download www.gov.uk/government/publications

Follow us on X: @educationgovuk
Connect with us on Facebook: facebook.com/educationgovuk