



Llywodraeth Cymru
Welsh Government

GUIDANCE

Protection of biometric information in schools and colleges

Guidance on your legal duties if you use biometric information.

First published: 13 August 2009

Last updated: 4 July 2022

This document was downloaded from GOV.WALES and may not be the latest version.

Go to <https://www.gov.wales/protection-biometric-information-schools-and-colleges-html> for the latest version.

Get [information on copyright](#).

Contents

[Introduction](#)

[Biometric data](#)

[The Protection of Freedoms Act 2012](#)

[Data Protection Act 2018 \(DPA 2018\) and the UK General Data Protection Regulation \(UK GDPR\)](#)

[Frequently asked questions](#)

[Associated resources](#)

[Letters and consent forms](#)

This document was downloaded from GOV.WALES and may not be the latest version.

Go to <https://www.gov.wales/protection-biometric-information-schools-and-colleges-html> for the latest version.

Get [information on copyright](#).

Introduction

This non-statutory guidance from the Welsh Government is intended to explain the legal duties schools and colleges have if they use 'automated biometric recognition systems'.

Expiry/review date

This advice will be kept under review and updated as necessary.

What legislation does this advice relate to?

- [The Protection of Freedoms Act 2012](#)
- [Data Protection Act 2018 \(DPA 2018\)](#)
- [UK General Data Protection Regulation \(UK GDPR\)](#)

Who is this advice for?

This advice is aimed at proprietors, governing bodies, headteachers and principals of all schools (including independent schools and all categories of maintained schools) and colleges. It will also be of use to school and college staff, parents, people other than a child's natural parents who have parental responsibility (such as carers) and learners.

Key points:

- Before schools and colleges decide to put in place a biometric system to collect data, careful and meaningful consideration should be made as to whether alternative and less intrusive options are available that can deliver

This document was downloaded from GOV.WALES and may not be the latest version.

Go to <https://www.gov.wales/protection-biometric-information-schools-and-colleges.html> for the latest version.

Get [information on copyright](#).

the equivalent level of services to learners.

- The use of biometric systems brings with it additional legal obligations under the legislations referenced above. Schools and colleges will also need to consider the **UN Convention on the Rights of the Child (UNCRC): UNICEF UK**. Under Article 12 children and young people have the right to express their views, feelings and wishes in all matters affecting them, and to have their views considered and taken seriously. Article 16 gives them a right to privacy. More information is included in the Children's Rights Impact Assessment section.
- Schools and colleges that use biometric recognition systems must treat the data collected with appropriate care and must comply with the data protection principles set out in the UK General Data Protection Regulation (UK GDPR), implemented by the Data Protection Act 2018 (DPA 2018), and the additional requirements in sections 26 to 28 of the Protection of Freedoms Act 2012.
- For learners under the age of 18, schools and colleges must ensure that all the parents/carers of the learner are notified and the written consent of at least one parent/carer is gained before a learner's **biometric data** is taken and processed for the purposes of any automated biometric recognition system. This applies to all learners in schools and colleges under the age of 18.
- Schools and colleges must not process the biometric data of a learner who objects or refuses to participate in the processing of their biometric data, or where a parent/carer has objected, or where no parent/carer has consented in writing to the processing of the biometric data.
- Schools and colleges must provide reasonable alternative means of accessing services for those learners who will not be using an automated biometric recognition system; and must ensure that it does result in the unequal treatment of learners.
- Schools and colleges should provide details of how they store a learner's biometric data if a request is received from that individual learner or from their parent/carer.

This document was downloaded from GOV.WALES and may not be the latest version.

Go to <https://www.gov.wales/protection-biometric-information-schools-and-colleges.html> for the latest version.

Get [information on copyright](#).

Biometric data

What is biometric data?

Biometric data is 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.

Biometric data is a special category data whenever it is processed "for the purpose of uniquely identifying a natural person". This means that biometric data will be special category data in the vast majority of cases. If schools or colleges use biometrics to learn something about an individual, authenticate their identity, control their access, make a decision about them, or treat them differently in any way, then the schools or colleges will need to comply with Chapter 2, Article 9 of the UK GDPR.

The Information Commissioner considers biometric data used for the purpose of uniquely identifying a natural person' as a special category data as listed as such in Article 9(1) of UK GDPR. This means that it must be obtained, used and stored in accordance with the Data Protection Act 2018 (see DPA 2018 below).

The Protection of Freedoms Act 2012 includes provision which relates to the use of this data in schools and colleges (see The Protection of Freedoms Act 2012 below).

What is an automated biometric recognition system?

An 'automated biometric recognition system' uses technology which measures an individual's physical or behavioural characteristics by means of equipment

This document was downloaded from GOV.WALES and may not be the latest version.

Go to <https://www.gov.wales/protection-biometric-information-schools-and-colleges-html> for the latest version.

Get [information on copyright](#).

operating automatically (i.e. electronically). Information from the individual is automatically compared with biometric information stored in the system in order to recognise or identify the individual.

Biometric systems currently used in schools and colleges are based on recognition technology, such as those listed above as 'biometric data'. Biometric systems usually store mathematical templates that allow physical characteristics to be recognised rather than images of the characteristics themselves; these templates are also biometric data. These systems can be used by schools and colleges for a number of purposes, for example: automated attendance and registration, meal payments and for borrowing books from libraries.

The decision on whether to introduce such biometric systems rests with individual schools and colleges. However, the Welsh Government recognises that the implementation of such systems in schools and colleges can be a sensitive issue and careful consideration must be given as to whether it is necessary and proportionate. As noted above in the key points, schools and colleges should consider all other options, which are less intrusive, before adopting a biometric system. A strategic **Data Protection Impact Assessment (DPIA)** will assist data controllers, usually governing bodies, through the issues that need to be considered in terms of lawfulness, proportionality and generic risks.

Where schools or colleges choose to install electronic registration systems, they are required to comply with the principles of the DPA 2018 and the UK GDPR, in relation to all personal data collected and held by them. This would include the use of biometric data as part of any management information system within the school or college.

As mentioned above, the use of biometric technology in schools or colleges is a sensitive issue. There is a risk that any school or college in the UK who decides to utilise biometric technology may be required to halt its use as existing legislation (that they are subject to) has deemed this in other areas of the EU.

What is Facial Recognition Technology (FRT)?

FRT is the process by which an individual can be identified, or otherwise recognised, from a digital facial image. One-to-one FRT is where individuals are aware of participating directly in the process. An example of where this may be considered for use in a school/college, is for entry into schools/colleges or to operate a cashless system in school canteens.

A different type of FRT is live facial recognition, which is less targeted and has greater potential to be used without the individual's knowledge, choice or control. It can capture the biometric data of all individuals passing within range of a video surveillance camera automatically and indiscriminately, similar to CCTV.

Information Commissioners Office (ICO)

The ICO is an independent body with responsibility for upholding information rights, and can offer further advice on the management of records and the handling of requests for information.

Schools and colleges should be mindful that the ICO has **raised concerns about the use of live facial recognition**. When considering any new use of personal data the UK GDPR requires that the data controller, which is normally the governing body, takes a '**data protection by design and default**' approach to ensure that compliance is embedded in the project from the start.

It is recommended that schools and colleges seek the advice of their data protection officer (DPO) before making any decision to proceed with use of biometric systems whilst mindful that legal responsibility for compliance with data protection laws rests with the data controller.

Any school or college intending on introducing FRT must undertake a full Data

Protection Impact Assessment (DPIA) and a Children's Rights Impact Assessment (see section CRIA), before the collection and processing of any biometric data.

Due to the sensitivity and intrusive nature of FRT, there are additional obligations a school or college must consider if they intend to use this technology. The use of biometric data for identification purposes is considered a special category data (under UK GDPR), therefore schools and colleges need to have identified a **lawful basis** for processing personal data under Article 6 and also a condition for processing special category data under Article 9.

It is recommended that schools and colleges who intend to adopt technological developments in this area become fully aware of the advice provided by the **Information Commissioner's Office (ICO)** and should consider engaging with the **Biometrics Commissioner for England and Wales** to ensure all considerations are adequately addressed.

We are not aware of any schools/colleges in Wales currently operating FRT systems and would strongly discourage the use of this technology. The **Surveillance Camera Code of Practice** has recently updated by the Home Office and local authorities are under a legal obligation to have regard to the statutory Code which regulates the use of surveillance camera systems in public places.

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 disclosing it, deleting it, organising it or altering it, please refer to section 1(3) of the DPA 2018. Schools/colleges will need to identify a lawful base for processing biometric information in relation to Article 6 of UKGDPR.

This document was downloaded from GOV.WALES and may not be the latest version.

Go to <https://www.gov.wales/protection-biometric-information-schools-and-colleges-html> for the latest version.

Get [information on copyright](#).

An automated biometric recognition system processes data when:

- recording learners' biometric data, for example, via a fingerprint scanner
- storing data relating to learners' fingerprints on a database system
- using the data as part of an electronic process which compares and matches biometric information in order to recognise learners

More information on these topics is also available via the [associated resources](#) section below.

Data processors

Suppliers of any biometric system will likely be 'data processors' for the use of pupil data, although this must be clarified on a case by case basis. Under Article 28 of UK GDPR, the controller must only use processors 'providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of [UK GDPR] and ensure the protection of rights of the data subject'. Article 28 specifies minimum [contractual requirements](#) that will comply with the law, in essence this ensures the processor can only act on instructions of the controller, and may not use the data for any other purposes. If a controller were to use a system without a fully compliant contract in place then that controller would likely bear full legal liability for the actions of the system provider, see our [contracts and liabilities guidance](#).

Schools/colleges should take extra care if considering any system where pupil data is to be disclosed to a third party controller, as once disclosed, this data would be outside of the school/college's control.

The Protection of Freedoms Act 2012

Notification and parental consent

Under the law, schools and colleges must notify all parents, including birth parents and those with parental responsibility for a child, of learners under the age of 18 where they intend to obtain and subsequently use their child's biometric information as part of an automated biometric recognition system. As long as the child does not object, and no parent objects in writing, the written consent of only one parent will be required.

Schools and colleges 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, where the whereabouts or identity of the parent is not known
- the parent lacks the capacity, as defined in the Mental Capacity Act 2005, to object or to consent to the processing of the child's biometric information; for example, where the parent has a mental impairment
- where the welfare of the child requires that the 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 the parent's 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 any of them):

- notification must be sent to all those who have care of the child and written consent must be gained from at least one carer unless the bullet point below applies
- where a child is looked after by a local authority or is accommodated or

maintained by a voluntary organisation, the consent of the local authority, or as the case may be, the voluntary organisation must be gained

Schools and colleges could, at the same time as enrolling a child, notify parents that they wish to take and then use their child's biometric information as part of an automated biometric recognition system and seek written consent to do so. In such circumstances, details of both parents should be requested by the school or college for both purposes (enrolment and notification of intention to process biometric information).

Under the **Education (Pupil Registration) (Wales) Regulations 2010**, 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 learner, including non-resident parents. Schools who wish to notify and seek consent to process a child's biometric information at any point after enrolment of a child at the school should, therefore, have contact details for most parents in the admission register. Schools should, however, 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, by asking 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, by making enquiries with the local authority or other agency).

Schools and colleges are not expected to engage the services of a 'people tracer' or detective agencies in doing so 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 (notification of a parent not required if the parent cannot be found).

Schools and colleges must ensure that they satisfy themselves of the identity of any parents giving their consent.

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

Notification sent to parents should include full information about the processing of their child's biometric information. This information should include details about the type of biometric information to be taken; how it will be used; the parent's and learner's right to refuse or withdraw their consent; and the schools duty to provide alternative arrangements for those learners whose information cannot be processed. A sample 'Notification and Consent' template is included at the end of this advice.

The learner's right to refuse

The Protection of Freedom Act 2012, Part 1 Chapter 2 (26)(5) states that if a learner of any age objects or refuses to participate (or to continue to participate) in anything that involves the processing of their biometric data for the purposes of an automated biometric recognition system, the school or college must ensure that the learner's data are not processed, regardless of any consent given by their parents.

Children and young people have rights under the **UN Convention on the Rights of the Child (UNCRC): UNICEF UK**. Under Article 12 they have the right to express their views, feelings and wishes in all matters affecting them, and to have their views considered and taken seriously. Article 16 gives them a right to privacy.

Schools and colleges should take steps to ensure that learners understand that they can object or refuse to allow their biometric data to be used and that, if they do so, the school or college will have to provide them an alternative way of accessing the relevant service. Parents/carers should also be told of their child's

right to object or refuse and encouraged to discuss this with their child.

Providing alternatives

Reasonable alternative arrangements must be provided for learners who do not use automated biometric recognition systems, either because their parents have refused consent or due to their own refusal to participate.

A child friendly version of this guidance is available.

Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulation (UK GDPR)

The UK data protection regime is set out in the DPA 2018, along with the UK GDPR. Almost anything to do with data counts as processing; including collecting, recording, storing, using, analysing, combining, disclosing or deleting it.

The DPA 2018 sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998, and came into effect on 25 May 2018. It was amended on 01 January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the UK's status outside the EU. It sits alongside and supplements the UK GDPR.

UK GDPR is the UK General Data Protection Regulation. It is a UK law which came into effect on 01 January 2021. It sets out the key principles, rights and obligations for most processing of personal data in the UK.

Schools and colleges as data controllers must process learners' personal data, including biometric data, in accordance with UK GDPR. The provisions in the

This document was downloaded from GOV.WALES and may not be the latest version.

Go to <https://www.gov.wales/protection-biometric-information-schools-and-colleges-html> for the latest version.

Get [information on copyright](#).

Protection of Freedoms Act 2012 are in addition to the requirements in the DPA with which schools and colleges must continue to comply.

The DPA 2018 is split into a number of different parts, which apply in different situations and perform different functions. It sets out three separate data protection regimes with the relevant part for schools and colleges being; Part 2: General processing (UK GDPR).

The principles of the DPA 2018 must be considered when a school or college is deciding whether to introduce a biometric system and deciding which system is most appropriate.

When processing a child's personal data, including any such data used for the purposes of automated biometric recognition systems, schools and colleges must:

- hold biometric data securely to prevent unauthorised or unlawful use of the data
- store biometric data for no longer than it is needed. A school or college should, therefore, destroy any data held on a biometric system once a learner no longer uses the system. For example, the data should be destroyed if the learner leaves the school or college, or if parents withdraw consent or the child no longer wishes to have his or her biometric data processed
- ensure that such data is used only for the purposes for which it is obtained and that it is not unlawfully disclosed to third parties
- for further practical advice see the associated resources section below including guides on data protection for schools and colleges

Data Protection Impact Assessment

Article 35 of the GDPR introduces the concept of a Data Protection

This document was downloaded from GOV.WALES and may not be the latest version.

Go to <https://www.gov.wales/protection-biometric-information-schools-and-colleges-html> for the latest version.

Get [information on copyright](#).

Impact Assessment (DPIA). DPIA is a tool to help you identify and minimise data protection risks. Conducting a DPIA meets, in parts, a school's or college's accountability obligations under GDPR, and is an integral part of the 'data protection by default and by design' approach. An effective DPIA helps you to identify and fix problems at an early stage, demonstrate compliance with your data protection obligations and meet learners' expectations of privacy.

A DPIA is a **statutory requirement** when the processing is "likely to result in a high risk to the rights and freedoms of natural persons" (Article 35(1)). You need to conduct a DPIA when processing data concerning vulnerable data subjects, which includes children (they can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data). A DPIA should also be used if implementing an innovative use of individual's data or applying new technological or organisational solutions, such as combining use of finger print and face recognition for improved physical access control.

If a decision is made to proceed with a new biometric system then that particular system will need to be evaluated by means of a DPIA to ensure full compliance with data protection law. This is the legal responsibility of the data controller (usually governing bodies).

Biometric system suppliers should be able to offer relevant information to support the data controller to discharge their legal function. Schools and colleges should not simply accept a pre-done DPIA from the supplier without satisfying themselves that the analysis fully meets their needs and accurately explores risks to the learner's data.

A DPIA does not have to eradicate all risk, but should help to minimise it and determine whether or not the level of risk is acceptable in the circumstances. Conducting a DPIA does not have to be complex or time-consuming in every case, but there must be a level of rigour in proportion to the privacy risks arising.

Where any DPIA shows residual high risk to the data subjects (in this case the

learner) despite mitigations, and where the controller still wishes to proceed with the proposal, Article 36(1) requires that they must submit their DPIA to the ICO for **prior consultation** before any processing of data commences.

The DPIA must address how the data controller can comply with all relevant data subject rights in relation to data that will be held on the biometric system.

There is no definitive DPIA template that must be followed. Schools/colleges can use a standard template or develop their own template and process to suit their particular needs. Further guidance and a sample template are available on the **ICO website** (ICO).

Children's Rights Impact Assessment (CRIA)

Children and young people have a right to be involved in decisions which affect them (Article 12 of the UNCRC). CRIA looks at proposals from children's perspective, measuring the impact on them against the articles of the UNCRC.

Any school or college intending to collect biometric information by using facial recognition technology should undertake a CRIA. It is a tool to be used in the planning process and provides for the systematic consideration of the direct or indirect impact that affects children and young people.

Undertaking a CRIA involves meaningful participation and engagement with children and young people, either by research data or through consultation. A CRIA should be evidence-based which will assist a school or college to assess the impact(s) of the proposal under consideration. It can also identify where gaps in the evidence base exist. One of the main purposes of a CRIA is to present a range of options that would comply with and/or better realise children's rights in the decision making process and by considering proportionality and necessity of any new biometric collection system.

CRIAs should include a monitoring and review mechanism, to prompt schools and colleges to revisit how their original aims have been met whilst respecting, protecting and fulfilling the rights of children and young people affected.

A completed CRIA should be made available in clear and plain English /Cymraeg Clir with information, advice and guidance for children, young people and families. This will give them an opportunity to consider and give informed consent to how their biometric data is being collected and stored.

Information and guidance on how to undertake a CRIA and a child rights impact assessment template for local authorities are available:

[A Children's Rights Approach in Wales: Children's Commissioner for Wales](#)

[Unicef: child friendly cities & communities](#)

Privacy information

Schools and colleges need to provide **privacy information that complies with UK GDPR**. This must be provided to the data subjects, in this case the learner, and where they are too young to be regarded as competent, to their parents/ carer. Schools and colleges will also need to produce an age appropriate version of the privacy information for younger data subjects. In practice, given the need for PoFA consent from parents of all age groups, it is likely to be beneficial to provide privacy information to all parents.

Frequently asked questions

What information should schools/colleges provide to

This document was downloaded from GOV.WALES and may not be the latest version.

Go to <https://www.gov.wales/protection-biometric-information-schools-and-colleges-html> for the latest version.

Get [information on copyright](#).

parents/learners to help them decide whether to object or to give their consent?

Schools and colleges should not attempt to persuade parents/carers to consent to the collection of biometric data. They should take steps to ensure parents/carers receive full information about the processing of their child's data including a description of the kind of system they plan to use, the nature of the sensitive data they process, what the purposes of the processing are and how the data will be obtained, used and stored.

If schools or colleges decide to implement new or enhanced biometric systems (such as Facial Recognition Technology), in providing details to parents/carers, they must also set out details of alternative mechanisms for the collection of learner data, that are equally easy and accessible for learners who choose not to provide consent for their biometric information to be collected in this way. This will enable any learner or parent to give informed **consent** to the collection of biometric data by this means or alternatively to object.

What if one parent disagrees with the other?

Schools and colleges will be required to notify all parents that they intend to take and process the child's biometric information. If one parent objects then the school or college will not be permitted to process the child's data.

How will the child's right to object work in practice, must they do so in writing?

No, the child is not required to object in writing. Whilst an older child may be able to say that they object to the processing of their biometric data, a younger child may show reluctance to take part in the physical process of giving the data. In

either case, the school or college will not be permitted to collect or process the data and will have to provide reasonable alternative arrangements to enable the child to access the relevant service.

What if a child requests that their parents are not contacted?

Schools and colleges must notify all parents of learners under the age of 18 where they intend to obtain and subsequently use their child's biometric information as part of an automated biometric recognition system. If a child requests that their parents are not contacted, schools and colleges may decide not to contact the child's parents. However, if all parents are not notified and consent cannot be obtained from parents whose consent is required, biometric information cannot be collected or processed.

Do local authorities have a right to refuse to allow schools to install biometric systems?

Governing bodies of maintained schools have the power in law to do anything which appears to them to be necessary or expedient for the purposes of, or in conjunction with, the conduct of the school. They, therefore, have the power to install a biometric system in their school for purposes such as improving the administrative efficiency of the school. The law does not require a governing body of a maintained school to obtain the expressed consent of the local authority to a proposal to install a biometric system in the school.

Are schools/colleges required to ask/tell parents before introducing an automatic biometric recognition system?

The law does not require schools and colleges to consult parents before installing an automated biometric system. However, for learners aged under 18 they are required to notify parents/carer and obtain explicit consent (Article 9 of the UKGDPR) before their child's biometric data is obtained or used for the purposes of such a system. It is up to schools and colleges to decide whether they think it is appropriate to consult parents and learners in advance of installing such a system.

Do schools need to renew consent every year?

No, the original written consent is valid until such time as it is withdrawn. However, if a parent or the child objects at any stage to the processing of the data, then the processing must cease. When the learner leaves the school or college, their data should be removed from the system.

Can consent be withdrawn by the learner or parent?

Parents of learners aged under 18 will be able to withdraw their consent, in writing, at any time. In addition, any other parent will be able to object, in writing, at any time to the processing of their child's data. The learner's right to refuse applies both to the giving of consent and the ongoing processing of biometric data. If at any time the learner objects to the processing of biometric data, the school or college must stop doing this immediately. The learner must be able to opt in and opt out with equal ease, and give explicit consent when changes are made to the method of collecting a learner's biometric information, or when there are changes planned for its use.

Will consent given on entry to primary or secondary school be valid until the child leaves that school?

Yes, consent will be valid until the child leaves the school. If at any point the parents or the child decide that the data should not be processed, they will have the right to have it stopped and removed from the school's system.

Can the school notify parents and accept consent via email?

Yes, as long as the school is satisfied that the email contact details are accurate and the consent received is genuine.

Will parents be asked for retrospective consent?

No, any processing that has taken place prior to the Protection of Freedoms Act 2012 coming into force will not be affected. However, any school or college that wishes to use, or to continue to use, automated biometric recognition systems will have to ensure that they have sent the necessary notifications to all parents and obtained the written consent from at least one parent before continuing or starting to use, such systems.

Does the legislation cover other technologies such a palm and iris scanning?

The legislation covers all systems which, by means of equipment operating, automatically record or use physical or behavioural characteristics for the purpose of identification. This will include systems which use palm, iris or face

recognition amongst others, as well as fingerprints.

Is parental notification and consent required for the use of photographs and CCTV in schools?

No, not unless the use of photographs and CCTV is for the purpose of an automated biometric recognition system. However, schools and colleges must adhere to the requirements in the DPA 2018 when using CCTV on their premises for general security purposes, or when using photographs of learners as part of a manual ID system or as part of an automated system that uses a barcode to provide a child with access to services. Depending on the circumstances of each case, consent may be required or be advisable under the Data Protection Act provisions. Photo ID card systems where a child's photograph is scanned to provide him or her with services would fall within the obligations on schools and colleges, under sections 26 to 28 of the Protection of Freedom Act 2012, as such systems fall within the definition in that Act of automated biometric recognition systems.

Is parental notification or consent required where a child uses or accesses standard commercial sites or software which use face recognition technology?

The provisions in the Protection of Freedom Act 2012 only cover the processing of biometric data by or on behalf of the school or college. If a school or college wishes to use such software for school/college work then the requirement to notify parents and to obtain parental consent will apply. However, if a learner is using this software for their own personal purposes then the provisions do not apply, even if the software is accessed using school or college equipment.

This document was downloaded from GOV.WALES and may not be the latest version.

Go to <https://www.gov.wales/protection-biometric-information-schools-and-colleges-html> for the latest version.

Get [information on copyright](#).

Associated resources

Welsh Government guidance for schools on communicating with parents and obtaining consent: [parents and parental responsibility: guidance for schools](#)

ICO guide to data protection: [UK GDPR guide](#) (ICO)

ICO guidance for education establishments: [schools, universities and colleges](#) (ICO)

Hwb resources: [a teacher's guide to the General Data Protection Regulation and what it means for your school](#)

Hwb resources: [data protection for schools and colleges](#)

Letters and consent forms

Schools and colleges will need to produce their own letter and consent form in order to request consent for the collection of a learner's biometric information.

The letter should be written in Plain English/Cymraeg Clir so it is accessible to all learners, parents and carers. It should provide absolute clarity for parents/carers and make them aware of the following:

- the requirements of sections 26-28 of the Protection of Freedoms Act 2012
- why and how you will be collecting the learner's biometric information
- that it is not mandatory to consent to the collection of a learner's biometric information and there are other options available which are equally as accessible, that will not disadvantage the learner
- that the written consent of at least one parent or a carer is required; that consent given by one parent will be overridden if the other parent objects in

This document was downloaded from GOV.WALES and may not be the latest version.

Go to <https://www.gov.wales/protection-biometric-information-schools-and-colleges-html> for the latest version.

Get [information on copyright](#).

writing to the use of their child's biometric information. Similarly, if the learner objects to this, the school or college cannot collect or use their biometric information for inclusion on any automated recognition system

- that the learner, parents or carers can opt out at any time and withdraw their consent for the collection and use of their biometric information
- that you will adhere to statutory requirements in relation to data protection impact assessments and children's rights impact assessments
- the retention period for holding biometric information for learners and when it will be destroyed
- that if you are planning changes to a biometric collection system, or changes to the use of the data collected, then you will request another formal consent for biometric information collection of the learner
- a link signposting learners, parents and carers to the Welsh Government's child and parent friendly version of this guidance.

Further information and guidance

- [ICO guide to data protection](#) (ICO)
- ["Parents" and "parental responsibility": guidance for schools](#)

Update coming soon.

This document may not be fully accessible.

For more information refer to our [accessibility statement](#).

This document was downloaded from GOV.WALES and may not be the latest version.

Go to <https://www.gov.wales/protection-biometric-information-schools-and-colleges-html> for the latest version.

Get [information on copyright](#).