RICARDS LODGE HIGH SCHOOL

Biometric Data Policy

PUBLISHED

October 2021

Ricards Lodge High School - Governing Board Approved Policy	
Date written/last review	October 2021
Approval level	Governing Body
Date of next review	October 2022
Add to website Y/N	Yes

Biometric Data Policy

Contents

What is biometric data?

1.1. Biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allows or confirms the unique identification of that natural person, such as facial images or dactyloscopic data.

1.2. The Information Commissioner considers all biometric information to be sensitive personal data as defined by the GDPR 2018; this means that it must be obtained, used and stored in accordance with that Regulation.

1.3. The Protection of Freedoms Act 2012 includes provisions which relate to the use of biometric data in schools and colleges when used as part of an automated biometric recognition system. These provisions are in addition to the requirements of the GDPR 2018.

2. What is an automated biometric recognition system?

2.1.An automated biometric recognition system uses technology which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (i.e. electronically). Information from the individual is automatically compared with biometric information stored in the system to see if there is a match in order to recognise or identify the individual.

2.2.Biometric recognition systems can use many kinds of physical or behavioural characteristics such as those listed in 1.1 above.

3. What does processing data mean?

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

a) Recording pupils' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner;

b) Storing pupils' biometric information on a database system; or

c) Using that data as part of an electronic process, for example, by comparing it with biometric information stored on a database in order to identify or recognise pupils.

Frequently Asked Questions

What information should schools provide to parents/pupils to help them decide whether to object or for parents to give their consent?

Any objection or consent by a parent must be an informed decision – as should any objection on the part of a child. Schools should take steps to ensure parents receive full information about the processing of their child's biometric data including a description of the kind of system they plan to use, the nature of the data they process, the purpose of the processing and how the data will be obtained and used. Children should be provided with information in a manner that is appropriate to their age and understanding.

What if one parent disagrees with the other?

Schools will be required to notify each parent of a child whose biometric information they wish to collect/use. If one parent objects in writing, then the school will not be permitted to take or use that child's biometric data.

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

A child is not required to object in writing. An older child may be more 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 other ways. In either case the school or college will not be permitted to collect or process the data.

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

Schools are not required by law to consult parents before installing an automated biometric recognition system. However, they are required to notify parents and secure consent from at least one parent before biometric data is obtained or used for the purposes of such a system. It is up to schools to consider whether it is appropriate to consult parents and pupils in advance of introducing 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, it can be overridden, at any time if another parent or the child objects to the processing (subject to the parent's

objection being in writing). When the pupil leaves the school, their biometric data should be securely removed from the school's biometric recognition system.

Do schools need to notify and obtain consent when the school introduces an additional, different type of automated biometric recognition system?

Yes, consent must be informed consent. If, for example, a school has obtained consent for a fingerprint/fingertip system for catering services and then later introduces a system for accessing library services using iris or retina scanning, then schools will have to meet the notification and consent requirements for the new system.

Can consent be withdrawn by a parent/carer?

Parents will be able to withdraw their consent, in writing, at any time. In addition, either parent will be able to object to the processing at any time but they must do so in writing.

When and how can a child object?

A child can object to the processing of their biometric data or refuse to take part at any stage – i.e. before the processing takes place or at any point after his or her biometric data has been obtained and is being used as part of a biometric recognition system. If a pupil objects, the school or college must not start to process his or her biometric data or, if they are already doing this, must stop. The child does not have to object in writing.

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

Yes. Consent will be valid until the child leaves the school – subject to any subsequent objection to the processing of the biometric data by the child or a written objection from a parent. If any such objection is made, the biometric data should not be processed and the school or college must, in accordance with the GDPR, remove it from the school's system by secure deletion.

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 provisions in the Protection of Freedoms Act coming into force will not be affected. Any school wishing to continue to process biometric data must have already sent the necessary notifications to each parent of a child and obtained the written consent from at least one of them before continuing to use their child's biometric data.

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

Yes. The legislation covers all systems that record or use physical or behavioural characteristics for the purpose of identification. This includes systems which use palm, iris or face recognition, as well as fingerprints.

Is parental notification and consent required under the Protection of Freedoms Act 2012 for the use of photographs and CCTV in schools?

No – not unless the use of photographs and CCTV is for the purposes of an automated biometric recognition system. However, schools and colleges must continue to comply with the requirements in the GDPR 2018 when using CCTV for general security purposes or when using photographs of pupils as part of a manual ID system or an automated system that uses barcodes to provide services to pupils. Depending on the activity concerned, consent may be required under the GDPR before personal data is processed.

The Government believes that the GDPR requirements are sufficient to regulate the use of CCTV and photographs for purposes other than automated biometric recognition systems. Photo ID card systems, where a pupil's photo is scanned automatically to provide them with services, would come within the obligations of schools and colleges under sections 26 to 28 of the Protection of Freedoms Act 2012, as such systems fall within the definition in that Act of automated biometric recognition systems.

Associated Resources

ICO guide to data protection

ICO guidance on data protection for education establishments

British Standards Institute guide to biometrics

RLHS Data Protection Policy

RLHS Privacy Notices (GDPR)