CAMBRIAN

Nurturing Growth - Inspiring Minds

Biometric Data Policy

V0.1

This document applies to all academies and operations of Cambrian Learning Trust.

www.cambrianlearningtrust.org

Document Control			
Author	Operations Manager	**Approved By**	QofE
Last Reviewed	22/09/2022	**Next Review**	22/09/2027
Review Cycle	5 years	**Version**	0.1

Contents

Background 3
What is Biometric Data? 3
Current Legislation 3
Data Protection 4
Key Points 4
Length of Consent 5
What is an automated biometric recognition system? 5
What does processing data mean? 6
Monitoring and Review of this Policy 6
Frequently Asked Questions 7

Background

Schools and colleges that use pupils' biometric data must treat the data collected with appropriate care and must comply with the data protection principles as set out in the General Data Protection Regulations (GDPR) 2018.

Cambrian Learning Trust (The Trust) has a pupil recognition system using biometrics which is used by Secondary pupils in the canteen. The Trust complies at all times with the Data Protection Act and with the provisions of the Protection of Freedoms Act 2012 regarding the use of biometric data.

Our biometric system significantly improves efficiency in the canteen as we operate a cashless catering system. This not only improves security for handling cash transactions in the school, it also reduces opportunities for bullying as there is nothing that can be stolen for use by another student. It improves productivity as there is a reduction in queuing time.

Our chosen solution allows us to use a secure database holding biometric data. This means we will store the least amount of data possible. This reduces the risk of loss of data. The data that is held cannot be used by any other agency for any other purpose.

The Trust will not use the biometric information for any purpose other than that stated above. The Trust will store the biometric information collected securely in compliance with the Data Protection Act 1998. The Trust will not share this information with anyone else and will not unlawfully disclose it to any other person.

What is Biometric Data?

Biometric information is information about someone's physical or behavioural characteristics that can be used to identify them. There are many possible biometrics, including for example, a digital photograph, fingerprint, or hand shapes. As part of our identity management systems, we will record a biometric measurement taken from a finger or thumb, but not a fingerprint image. The information is stored in a highly secure database and will only be used by the school to confirm who is using a range of services.

Current Legislation

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.

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.

This legislation requires the Trust to:

- Inform parents about the use of the biometric systems in the school and explain what applications use biometrics.
- Receive written permission from one parent if the school is to process biometric information for their child.
- Allow children to choose an alternative way of being identified if they wish.
- Children under 18 who do not have permission by September 2013 will not be able to use existing or new biometrics when using services in the school.

Data Protection

Schools within The Trust that use pupils' biometric data must treat the data collected with appropriate care and must comply with the data protection principles as set out in the Data Protection Act 1998. Where the data is to be used as part of an automated biometric recognition system, schools must also comply with the additional requirements in sections 26 to 28 of the Protection of Freedoms Act 2012.

Schools within The Trust must ensure that each parent of a child is notified of the school's intention to use the child's biometric data as part of an automated biometric recognition system. The written consent of at least one parent must be obtained and applies to all pupils in schools and colleges under the age of 18.

Schools must provide reasonable alternative means of accessing services for those pupils who will not be using an automated biometric recognition system.

Key Points

- Schools and colleges that use pupils' biometric data must treat the data collected with appropriate care and must comply with the data protection principles as set out in the General Data Protection Regulations (GDPR) 2018.

- Where the data is to be used as part of an automated biometric recognition system, schools and colleges must also comply with the additional requirements in sections 26 to 28 of the Protection of Freedoms Act 2012
- The Academy must ensure that each parent of a child is notified of the Academy's intention to use the child's biometric data as part of an automated biometric recognition system.
- The written consent of at least one parent must be obtained before the data is taken from the child and used ie, 'processed'. This applies to all pupils in schools and colleges under the age of 18. In no circumstances can a child's biometric data be processed without written consent.
- Schools and colleges must not process the biometric data of a pupil (under 18 years of age) where:
    - The child (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data;
    - No parent has consented in writing to the processing; or
    - A parent has objected in writing to such processing, even if another parent has given written consent.
- Schools and colleges must provide reasonable alternative means of accessing services for those pupils who will not be using an automated biometric recognition system.

Length of Consent

The original written consent is valid until such time as it is withdrawn. However, it can be overridden, at any time either parent/carer or the pupil themselves objects to the processing (subject to the parent's/carer's objection being in writing).

When the student leaves the school or academy, their biometric data will be securely removed from the academy's biometric recognition system.

What is an automated biometric recognition system?

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.

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

What does processing data mean?

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

- Recording pupils' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner;
- Storing pupils' biometric information on a database system; or
- 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

Monitoring and Review of this Policy

The Governing Committee or Trustees shall be responsible for reviewing this policy from time to time to ensure that it meets legal requirements and reflects best practice.

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 and colleges 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 and colleges will be required to notify each parent of a child whose biometric information they wish to collect/use. However, consent given by one parent will be overridden if the other parent objects in writing. The trust will then 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?

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 primary or 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?

No – Forms must be signed and returned. They are then kept on file for the duration of the student on role.

Does the legislation cover other technologies such a 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 on 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.

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

The provisions in the Protection of Freedoms Act 2012 only cover processing by or on behalf of a school or college. If a school or college wishes to use such software for school work or any school business, then the requirement to notify parents and to obtain written consent will apply. However, if a pupil 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.