Kendrick School

Biometric Data Policy

Approval Date: December 2022

Next Review Date: December 2024

Version: BDP V1 2020	
Version: BDP V2 2022	

Biometric Data Policy

Introduction

Kendrick School is committed to protecting the personal data of all its students and staff, including any biometric data collected and processed.

Biometric data is collected and processed in accordance with relevant legislation and guidance to ensure the data and the rights of individuals are protected.

This policy outlines the procedures Kendrick School follows when collecting and processing biometric data.

Legal Framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Protection of Freedoms Act 2012 sections 26 to 28
- Data Protection Act 2018
- General Data Protection Regulation (GDPR)
- DfE (2018) 'Protection of biometric information of child in schools and colleges'

This policy operates in conjunction with the following policies:

- Data Protection Policy
- Records Management Policy

School Responsibilities

Kendrick School will ensure:

- Students' biometric data will be treated with appropriate care and 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, the school will comply with the additional requirements in sections 26 to 28 of the Protection of Freedoms Act 2012.
- Each parent of a student is notified of the school's intention to use the student's biometric data as part of an automated biometric recognition system.
- Written consent of at least one parent is obtained before the data is taken from the student and used i.e, 'processed'. This applies to all students under the age of 18. In no circumstances can a student's biometric data be processed without written consent.

Kendrick School will not process the biometric data of a student (under 18 years of age) where:

a) The student (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data;

b) No parent has consented in writing to the processing; or

c) A parent has objected in writing to such processing, even if another parent has given written consent.

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 confirms the unique identification of that natural person, such as facial images or dactyloscopic (fingerprint) 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.

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 (see section 1.1)

Processing biometric data

'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 students' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner;

b) Storing students' 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 students.

Data Protection Principles

Kendrick School processes all personal data, including biometric data, in accordance with the key principles set out in the GDPR.

Kendrick School ensures biometric data is:

- Processed lawfully, fairly and in a transparent manner.
- Only collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date, and that reasonable steps are taken to ensure inaccurate information is rectified or erased.
- 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.
- Processed in a manner that ensures appropriate security of the information, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
-

As the data controller, Kendrick School is responsible for being able to demonstrate its compliance with the provisions outlined above.

Data Retention

Biometric data will be retained by the school and is valid until the student leaves the school – subject to any subsequent objection to the processing of the biometric data by the student or a written objection from a parent.

Alternative Arrangements

Parents, students, and staff members have the right to not take part in Kendrick School's biometric system(s).

Where an individual objects to taking part in the school's biometric system(s), reasonable alternative arrangements will be provided that allow the individual to access the relevant service.

Alternative arrangements will not put the individual at any disadvantage or create difficulty in accessing the relevant service or result in any additional burden being placed on the individual (and the student's parents, where relevant)

Frequently Asked Questions

What information should schools provide to parents/students 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 student. Schools and colleges should take steps to ensure parents receive full information about the processing of their student'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. Students 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 student whose biometric information they wish to collect/use. If one parent objects in writing, then the school or college will not be permitted to take or use that student's biometric data.

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

A student is not required to object in writing. An older student may be more able to say that they object to the processing of their biometric data. A younger student 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 student objects to the processing (subject to the parent's objection being in writing). When the student 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 or 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 student object?

A student 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 student 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 student does not have to object in writing.

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

Yes. Consent will be valid until the student leaves the school – subject to any subsequent objection to the processing of the biometric data by the student 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 or college wishing to continue to process biometric data must have already sent the necessary notifications to each parent of a student and obtained the written consent from at least one of them before continuing to use their student's biometric data.

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 student 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 student 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.

Associated Resources

ICO guide to data protection

ICO guidance on data protection for education establishments

British Standards Institute guide to biometrics