Protection of Biometric Data Policy

Proverbs 18:15

An intelligent heart acquires knowledge and the ear of the wise seeks knowledge.

The Governors are committed to supporting the school in its endeavours and to ensuring that this policy is achieved in the light of its vision,

Derby Cathedral School is a community that welcomes students, families and visitors of all faiths and none. The diversity and richness of such a family brings depth and a vibrancy to our core. Underpinning and permeating our community are fundamental Christian values, of which we are proud. In line with the teachings of the Church of England we ask;

"for individuals to be the best they can be".

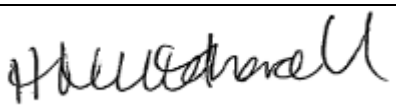
We ask that all stakeholders of Derby Cathedral School uphold this philosophy through

their ACTIONS,

their ASPIRATIONS,

and their ACHIEVEMENTS.

Through our curriculum, our enrichment opportunities, our pastoral House programme, our guidance and our role modelling, we aim to enable all members of our community to fulfill and exceed their potential.

Policy Status	Date	Chair of Governors	Review Date
Approved by LGB	17/10/2019		Autumn Term 20

Protection of Biometric Information of Children in Schools

What is biometric data?

Biometric data means personal information about an individual's physical or behavioural characteristics which can be used to identify that person; this may include their fingerprints, facial shape, retina and iris patterns, and hand measurements. The Information Commissioner considers all biometric information to be personal data as defined by the Data Protection Act 1998; this means that it must be obtained, used and stored in accordance with that Act (see the Data Protection Act 1998 below). The Protection of Freedoms Act 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 Data Protection Act 1998 (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 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 in 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 students' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner;

• storing students' 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 students.

How will we use the information?

The biometric fingerprint information which we are referring to above is used by Derby Cathedral School to provide a cashless catering service in the School.

How do I give or deny consent?

Derby Cathedral School has a form for this purpose. If you have not received the form another copy is available by contacting the School Business Manager j.foulkes@derbycathedralschool.org.uk

What if I do not wish to give consent to Derby Cathedral's School use of my child's biometric data?

If consent is not provided, the School has to provide an alternative way for your child to use the facilities managed by the biometric data. In Derby Cathedral School's case, for cashless catering, this will be by the use of a 4-digit PIN number which will have to be input at the point of sale.

Legislation

What legislation does this advice relate to?

- The Protection of Freedoms Act 2012
- The Data Protection Act 1998

Key points

Schools and colleges which use students' 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 and colleges must also comply with the additional requirements in sections 26 to 28 of the Protection of Freedoms Act 2012. Schools and colleges must ensure that parents are 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 before the data is taken from the child and used (i.e. 'processed'). This applies to all students in schools and colleges under the age of 18. In no circumstances may a child's biometric data be processed without written consent.

Schools and colleges must not process the biometric data of a student (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

- one 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 students who will not be using an automated biometric recognition system.

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 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.

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 students 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 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 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 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 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 Data Protection Act, 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.

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

Yes. The legislation covers all systems which 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 Data Protection Act 1998 (DPA) when using CCTV for general security purposes or when using photographs of students as part of a manual ID system or an automated system which uses barcodes to provide services to students. Depending on the activity concerned, consent may be required under the DPA before personal data is processed. The Government believes that the DPA 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 student's photo is scanned automatically to provide him or her 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.