CHOLLERTON CHURCH OF ENGLAND AIDED FIRST SCHOOL

Be the best you can be through:

challenge, nurture, inspiration, respect, happiness, inclusion, in a safe, loving Christian family.

Protection of Biometric Information POLICY

About this advice
This is non-statutory advice from the Department for Education. It is intended to explain the legal duties schools and colleges have if they use automated biometric recognition systems.

This advice replaces "Becta guidance on biometric technologies in schools".

What legislation does this advice relate to?
The Protection of Freedoms Act 2012
The Data Protection Act 1998

Who is this advice for?
This advice is aimed at proprietors, governing bodies, head teachers and principals of all schools, sixth form colleges and 16-19 Academies It will also be of use to school and college staff, parents and pupils.

Key points

- Schools and colleges that use, or could potentially use in the future, biometric recognition systems (see 2 below) must treat the data collected with appropriate care and must comply with the data protection principles set out in the Data Protection Act 1998.
- Schools and colleges must ensure that all the parents of a child are notified and the written consent of at least one parent is gained before a pupil's biometric data (see 1 below) is taken and processed further (see 3 below) for the purposes of an automated biometric recognition system. This applies to all pupils in schools and colleges under the age of 18.
- Schools and colleges must not process the biometric data of a pupil (under 18 years of age) who objects or refuses to participate in the processing of their biometric data. They must also not process such data where a parent has objected or no parent has consented in writing to the processing.
- Schools and colleges must provide reasonable alternative means of accessing services for those pupils who will not be using an automated biometric recognition system.

What is biometric data?

1. 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. This does not include photographs, other than where a child's photograph is automatically scanned by an automated biometric recognition system to provide him or her with a service in the school.
2. The Information Commissioner considers all biometric information to be personal information under 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).
3. The Protection of Freedoms Act includes provisions which relate 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 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 1) above.

<u>THE PROTECTION OF FREEDOMS ACT 2012</u>

Parental Consent

What the law says:

1. Schools and colleges must notify all parents of pupils under the age of 18 where they intend to take and subsequently use their child's biometric data. As long as the child does not object and no parent objects in writing, the written consent of only one parent will be required for a school or college to process the child's biometric information.
2. Schools and colleges will not need to notify a particular parent or seek his or her consent if the school or college is satisfied that:
    a. the parent cannot be found, for example where the whereabouts or identity of this particular parent is not known;
    b. the parent lacks the capacity to object or to consent, for example where he or she is mentally ill;
    c. where the welfare of the child requires that this particular 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; or
    d. where it is otherwise not reasonably practicable for this parent's consent to be obtained.

3. Where none 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):
    a. unless paragraph (b) below applies, notification must be sent to all those caring for a child and written consent must be gained from at least one carer;

b. 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.

4. Schools and colleges could, at the same time as enrolling a child, notify parents that they intend 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. Details of both parents should be requested by the school or college for both purposes (enrolment and notification of intention to process biometric information).

5. Under the Education (Pupil Registration) Regulations 2006, schools are required to keep an admissions register that includes the name and address of every person known to the school to be a parent of the child, including non-resident parents. Schools that wish to notify and seek consent to process a child's biometric information at any point after the 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).

6. Schools and colleges are not expected to engage the services of '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 2. a) (notification of a parent not required if the parent cannot be found).

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

8. 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 parents' and the pupil's right to refuse or withdraw their consent; and the school's duty to provide alternative arrangements for those pupils whose information cannot be processed.

The pupil's right to refuse

What the law says:

1) If a pupil of any age under 18 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 pupil's data is not processed regardless of any consent given by their parents.

Also note

2) Schools and colleges should take steps to ensure that pupils 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 with an alternative way of accessing the relevant service. Parents should also be told of their child's right to object or refuse and encouraged to discuss this with their child.

Providing alternatives

What the law says:

1) Reasonable alternative arrangements must be provided for pupils who do not use automated biometric recognition systems either because their parents have refused consent or due to their own refusal to participate in the collection of the biometric data.

<u>THE DATA PROTECTION ACT 1998</u>

1) Schools and colleges as data controllers must process pupils' personal data, including biometric data, in accordance with the Data Protection Act 1998 (DPA). The provisions in the Protection of Freedoms Act 2012 are in addition to the requirements in the DPA with which schools and colleges must continue to comply.
2) The DPA has eight principles with which all data controllers must comply.
3) When processing a child's personal data, including any such data used for the purpose of automated biometric recognition systems, schools and colleges must:
    a. Hold biometric data securely to prevent unauthorised or unlawful use of the data.
    b. 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 pupil no longer uses the system. For example, the data should be destroyed if the pupil leaves the school or college, if parents withdraw consent or the child no longer wishes to have his or her biometric data processed.
    c. 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.

Date approved by the Governing Body:
Signed by -
Ummu Feeley
.....
This policy was reviewed: Autumn 2023
Date of next review: Autumn 2024