BIOMETRIC DATA POLICY

Reviewed and updated: May 2021
Next review: September 2022

This policy is about the protection of the biometric information of children and relates to the following legislation:

- The Protection of Freedoms Act (PFA) 2012.
- The General Data Protection Regulation (GDPR) 2018 and the Data Protection Act 2018 (together hereinafter referred to as the 'Data Protection Laws').

It should be read in conjunction with each school's General Data Protection Regulation (GDPR) policy, as well as any compliant Data protection policy and Data security policy.

Advice for proprietors, governing boards, headteachers, principals and school and college staff is contained in the DFE non-statutory advice dated March 2018 and entitled 'Protection of biometric information of children in schools and colleges'.

Definitions

In order to understand the terminology used in this policy, the following definitions are explained.

Biometric data

- This is personal information about a person's physical, physiological or behavioural characteristics that can be used to identify that person. This can include their fingerprints, palm or fingertip characteristics, facial shape, retina and iris patterns and hand measurements.
- All biometric information is considered by the Information Commissioner to be personal data as defined by the GDPR 2018. This means it must be obtained, used and stored in accordance with those regulations.
- The PFA 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 data protection laws.

Automated biometric recognition system

- This is technology which measures an individual's physical or behavioural characteristics by means of equipment that operates 'automatically' (ie electronically) and uses this information in order to recognise or identify them.

- Biometric recognition systems can use many kinds of physical, physiological or behavioural characteristics such as fingerprints, facial images or hand measurements etc.

Processing data

This means 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:

- Recoding pupils' biometric data – for example taking measurements from a fingerprint via a fingerprint scanner.

- Storing pupils' biometric information on a database system.

- 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.

Key points

The following is a summary of the essential elements of this policy. More details are contained in the frequently asked questions section that follows.

- Schools that use biometric recognition systems must treat the data collected with appropriate care and must comply with the data protection principles set out in the data protection laws.

- Schools must ensure that all the parents of a child are notified and the written consent of at least one parent is gained before a child's biometric data is taken and processed further for the purposes of an automated biometric recognition system. This applies to all pupils in schools under the age of 18.

- Schools must not under any circumstances process the biometric data of a pupil who objects or refuses verbally or non-verbally to participate in the processing of their biometric data. They must also not process such data where a parent has objected (even if another parent has given written consent) or no parent has consented in writing to the processing.

- Schools must provide reasonable alternative means of accessing services for those pupils who will not be using an automated biometric recognition system. These arrangements should ensure that pupils do not suffer any disadvantage or difficulty in accessing services as a result of not participating in the system. Likewise such arrangements should not place any additional burden on parents whose children are not participating in such a system.

- **There is an issue concerning the use of fingerprint or fingertip identification processes during the current coronavirus (COVID-19) outbreak, as there is a concern about the health risks (transmission of the virus) of large numbers of pupils using the same machines. St John Bosco College has suspended the use of fingertip identification and has switched to contactless cards only temporarily. If there is a decision to switch to another method, then it would be necessary to seek parental/pupil agreement to the change and the same rules as outlined below would apply (see FAQ 6).**

Frequently asked questions

1. What information should schools provide to parents and pupils to help them know whether to object or give their consent?

Any objection or consent by a parent must be an informed decision as should any objection on the part of the 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 that they intend 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 way that is appropriate to their age and understanding.

However, the PFA does give details of special circumstances where schools and colleges do not need to notify a particular parent or seek his or her consent (eg the parent cannot be found, or there is a question of parental mental capacity or the welfare of the child might be adversely affected if a parent is contacted). It also explains (section 28) what happens if a child is looked after by their local authority (LA) or a voluntary organisation.

2. What if one parent disagrees with the other?

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

3. How will the child's right to object work in practice?

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 will not be permitted to collect or process the data. A pupil's objection or refusal overrides any parental consent to the processing.

4. 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.

5. 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.

6. 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, the school has obtained consent for a fingerprint or fingertip system for catering services and then 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.

7. Can consent be withdrawn by a parent or child?

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. The child's right to refuse

applies both to the giving and the on-going processing of biometric data. If at any time the child objects to the processing of biometric data, the school or college must stop doing so. The child does not have to object in writing.

8. Will consent given on entry to secondary school be valid until that child leaves the school?
Yes, consent will be valid until the child leaves that school. If at any point the parents or child decide that the data should not be processed they will have the right to have it removed from the school's system by secure deletion.

9. Can the school notify parents and accept consent by email?
Yes, as long as the school is satisfied that the email contact details are accurate and the consent received is genuine.

10. Does the legislation cover all biometric technologies?
Yes, the legislation covers all systems that record physical, physiological or behavioural characteristics.

11. Is parental notification and consent required under the PFA 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 requirements of the GDPR 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 data protection laws before personal data is processed. The government believes that the requirements of the data protection laws are sufficient to regulate the use of CCTV and photographs for purposes other than biometric recognition systems. Photo ID card systems, where a pupils' photo is scanned automatically to provide them with services, would come under the obligations placed on schools and colleges under sections 26 to 28 of the PFA, because such systems fall within the definition in that Act of automated biometric recognition systems.

12. Is parental notification or consent needed if a pupil uses or accesses standard commercial sites or software which uses facial recognition technology?
The provisions in the PFA only cover processing by or on behalf of a school or college. If the school or college wishes to use software for school work or school business then the requirement to notify parents and to obtain written consent will apply. However, if the pupil is using the software for their own personal purposes, the provisions do not apply, even if the software is accessed using school or college equipment.

Associated resources

- ICO general guidance on data protection.
- ICO guidance on data protection for educational establishments.
- British Standards Institute guide to biometrics.

MODEL CONSENT FORM FOR THE USE OF BIOMETRIC

INFORMATION IN SCHOOL

Please complete this form if you consent to your child using the biometric systems at [St John Bosco College] for current or future use of the [cashless catering, library management, printing, door access, lockers and e-registration] until s/he leaves the school/college.

Once your son/daughter ceases to use the biometric recognition system, his/her biometric information will be securely and permanently deleted by the school.

I/We acknowledge receipt of the information about use of biometric data at the school.

I/We give consent to the school for the biometrics of

Name…….

to be used at [St John Bosco College] as part of a recognition system as described above.

I/We understand that I/we can withdraw this consent at any time in writing.

Name of
parent(s)……..

Signature(s)……

Date
……..