Blackfen School for Girls

Protection of Biometric Information Policy

Head Teacher: Mr M Brown
Chair of Governors: Mr S Fitz-Gerald

	Date	Name	Signature
Policy Date	February 2020		
Review Date	February 2021		
Review Period	Annually		
Lead Person	Business Manager	Gary Morgan	
Prepared by	Business Manager	Gary Morgan	
Verified by	Head Teacher	Matthew Brown	
Approved by	Chair of Governors	Stuart Fitz-Gerald	

Contents

Introduction

1.1 Schools and colleges that use pupils' biometric data (see 1 below) must treat the data collected with appropriate care and must comply with the data protection principles as set out in the General Data Protection Regulation 2016 (GDPR) and the Data Protection Act 2018 (DPA).

1.2 Where the data is to be used as part of an automated biometric recognition system (see 2 below), schools and colleges must also comply with the additional requirements in sections 26 to 28 of the Protection of Freedoms Act 2012.

1.3 Blackfen School must ensure that each parent of a student is notified of Blackfen School's intention to use the student biometric data (see 1 below) as part of an automated biometric recognition system.

1.4 The written consent of at least one parent must be obtained before the data is taken from the student and used (i.e. 'processed' – see 3 below). This applies to all pupils in schools and colleges under the age of 18. In no circumstances can a student biometric data be processed without written consent.

1.5 Blackfen School must not process the biometric data of a pupil (under 18 years of age) where:

- The student (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.

1.6 Blackfen School must provide reasonable alternative means of accessing services for those pupils who will not be using an automated biometric recognition system. This is provided in the form of a PIN number.

What is biometric data?

2.1 Biometric data means 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.

2.2 Biometric data is classified as Special Category data under the GDPR and DPA. A lawful basis for processing under Article 9 of GDPR must be identified by the school. For the purposes of this document, the lawful basis is Article 9(2)(a) Consent.

2.3 Biometric data must be obtained, used and stored in accordance with the GDPR and DPA.

2.4 In line with GDPR requirements, a Privacy Impact Assessment must be carried out before the biometric data system is implemented, assessing any risks to data subjects and the measures the GDPR School will take to minimise the risks.

2.5 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 Data Protection Act 1998 and 2018.

What is an automated biometric recognition system?

3.1 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.

3.2 Biometric recognition systems can use many kinds of physical or behavioural characteristics such as those listed in 1) above.

What does data processing mean?

4.1 '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.

Biometric data use at Blackfen School

Consent for biometric data use is sought when a pupil joins the school. The consent is logged in SIMS and can be withdrawn at any time as stated on the consent form.

Finger-image data is held onsite on a secure server and is retained for the duration of the student time at the school. Finger-image data is used exclusively for the use of the school canteen (Fastrak Cashless Catering Software).

Frequently Asked Questions

What is biometric data?
Biometric data means personal information about an individual's physical or behavioural characteristics that can be used to identify that person; this can include their finger-images, facial shape, retina and iris patterns, and hand measurements.

For the purposes of Blackfen School, this takes the form of a finger-image used to identify users when they purchase school meals.

Biometric data (finger-images) are stored as a series of data points, converted from images by a mathematical algorithm. These data points cannot be used to reconstruct a useable fingerprint even with the algorithm available. The level of detail stored in these data points is well below the level of detail needed for forensic identification of someone and would be completely inadmissible, both in terms of quality and legality, in court. The data points are encrypted before being stored. The encryption standard used by the system in place at Blackfen School (BioStoer) for encrypting the data points is AES 256 with the symmetric key being stored in RSA 2048.

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 or pupil must be an informed decision. Blackfen School will take steps to ensure parents and pupils receive full information about the processing of biometric data including a description of the kind of system in use, the nature of the data processed, the purpose of the processing and how the data will be obtained and used. Pupils 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
will not be permitted to take or use that student biometric data.

How will the student 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 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 finger-image 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 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 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 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 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.

Will parents be asked for retrospective consent?
No. Any processing that took place prior to the provisions in the Protection of Freedoms Act coming into force is not affected. After 1 September 2013 (when the new duties in the Act took effect), any school or college wishing to continue to process biometric data from that date 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 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 Data Protection Act 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 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 pupil'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 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.

Associated Resources

- DfE guidelines for Protection of Biometric Information of Children in Schools https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/268649/biometrics_advice_revi sed_12_12_2012.pdf
- DfE guidelines for schools on communicating with parents and obtaining consent: https://www.gov.uk/government/publications/dealing-with-issues-relating-toparental-responsibility
- British Standards Institute guide to biometrics: http://shop.bsigroup.com/en/Browse-by-Subject/Biometrics/?t=r

Equality Impact Assessment

We have a duty to consider the impact of changes on groups with Protected Characteristics (race, disability, age, sex, sexual orientation, religion or belief, gender reassignment, pregnancy and maternity, marriage and civil partnership). An EIA needs to consider:

- Would the change impact differentially on pupils/ staff with protected characteristics? Positively or negatively?
- How do I know that?
- What could I do to mitigate any differential or negative impact?
- Is this still the right thing to do?

1. **What are the overall aims of the change? Why is the School proposing it?**
   The aim of this policy is to provide a framework to ensure that the policy has the procedures and guidelines in place to ensure that all stakeholders are fully supported.

2. **Given the aims of the proposal, what issues does the data/information highlight?**
   Everybody is included within this policy, and all groups are given equability in regard to their needs and provisions.

3. **How could the proposed change impact positively/negatively on groups with protected characteristics?**
   This has a positive impact on all groups with protected characteristics as they are ensured equal treatment and provision based on their needs. Risk assessments may be carried out to ensure that this is the case and provisions maybe altered to accommodate specific needs.

4. **What actions will we take to mitigate any negative impact?** No negative impact to having this policy.

5. **Is any potential negative impact justified in the light of the wider benefits of the proposal?**
   No negative impact to having this policy.

6. **Recording of final decision**
   This policy will be approved by the Governing Body.