



**HuishEpiscopi**

## **ACADEMY PROCEDURE**

### **Biometric Data Policy**

**July 2022**



Document title				
BIOMETRIC DATA POLICY				
Status			Committee/Board	
Academy Procedure			Full Board	
Review date			Date adopted	
Annually July 2023			05 July 2022	
For public access on request <i>Tick as appropriate</i>			Lead Academy Staff/Director	
Post		Online		The Principal/Business Manager
Notes				

## Contents

1. Introduction
2. What is biometric data?
3. What is an automated biometric recognition system?
4. What does data processing mean?
5. Biometric data use at Huish Episcopi Academy.
6. Frequently Asked Questions
7. Associated Resources
8. Equality Impact Assessment

## Introduction

- 1.1 Huish Episcopi Academy will treat the biometric data collected with appropriate care and will 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), Huish Episcopi Academy will also comply with the additional requirements in sections 26 to 28 of the Protection of Freedoms Act 2012.
- 1.3 Huish Episcopi Academy must ensure that each parent of a child is notified of Huish Episcopi Academy's intention to use the child's biometric data 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 child and used (i.e. 'processed'). This applies to all students in Academy under the age of 18. In no circumstances can a child's biometric data be processed without written consent.
- 1.5 Huish Episcopi Academy 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
  - A parent has objected in writing to such processing, even if another parent has given written consent.

- 1.6 Huish Episcopi Academy must provide reasonable alternative means of accessing services for those students who will not be using an automated biometric recognition system.

## **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 Academy. 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 Huish Episcopi Academy 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 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.

## **Biometric data use at Huish Episcopi Academy**

- 5.1 Huish Episcopi Academy use a cashless catering system in the Academy's dining hall, which includes biometric readers as a method of identifying an individual person.

The system uses an algorithm based scan, which reads between 50 and 130 points on the finger/thumb. It is not a fingerprint in any way, shape or form and is of use only in the cashless system.

The information of a student or staff member, who has been biometrically registered, is stored on a secure biometric controller within the Academy, which only your provider can access with permission from the Academy. Once an account has been created, the student or staff member places their finger/thumb on the biometric reader, which looks up their account and allows them to purchase items using only this method of identification.

Parental consent must be obtained before an individual's finger/thumb scan can be taken. A biometric consent form is included in the new student admissions pack.

## **Frequently Asked Questions**

### **What information should the Academy 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. Huish Episcopi Academy will 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. Students will be provided with information in a manner that is appropriate to their age and understanding.

### **What if one parent disagrees with the other?**

Huish Episcopi Academy will notify each parent of a child whose biometric information they wish to collect/use. If one parent objects in writing, then the Academy will not be permitted to take or use that child's biometric data.

### **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 Academy will not be permitted to collect or process the data.

### **Is the Academy required to ask/tell parents before introducing an automated biometric recognition system?**

The Academy is not required by law to consult parents before installing an automated biometric recognition system. However, the Academy is 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 the Academy to consider whether it is appropriate to consult parents and students in advance of introducing such a system.

**Does the Academy 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 will be securely removed from the school's biometric recognition system.

**Does the Academy need to notify and obtain consent when it introduces an additional, different type of automated biometric recognition system?**

Yes, consent must be informed consent. If, for example, the Academy 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 the Academy 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 the Academy be valid until the child leaves the Academy?**

Yes. Consent will be valid until the child leaves the Academy – 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 Academy, in accordance with the Data Protection Act, will remove it from the Academy's system by secure deletion.

**Can the Academy notify parents and accept consent via email?**

Yes – as long as the Academy 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 child and obtained the written consent from at least one of them before continuing to use their child'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 Data Protection Act 2018 when using CCTV for general security purposes or when using photographs of students as part of a manual ID system or an automated system that 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.

## **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\\_revised\\_12\\_12\\_2012.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/268649/biometrics_advice_revised_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-to-parentalresponsibility>
- British Standards Institute guide to biometrics: <http://shop.bsigroup.com/en/Browse-by-Subject/Biometrics/?t=r>

## **Equality Impact Assessment (EIA)**

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 students/ 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 Academy 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 go to Directors for approval