Wigston Academies Trust

PROTECTION OF BIOMETRIC INFORMATION OF CHILDREN: STATUTORY

DATE APPROVED:	6th December 2021
APPROVED BY:	Board of Trustees
REVIEW FREQUENCY:	Annually
DATE FOR REVIEW:	December 2022

Signed by Chair of Trust  Date: 6th December 2021

CONTENTS

1. INTRODUCTION

At the time of writing this policy, Wigston Academies Trust is using biometric data in a very limited way. The canteen system has moved away from finger recognition to a PIN system and the Academy library uses finger identification but this is under review. However, it is a statutory requirement to hold this policy and it will be applied if the Trust increases its use of biometric data for school systems in the future.

2. KEY GUIDANCE

2.1 Schools and colleges that 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 General Data Protection Regulations (GDPR) 2018.

2.2 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**.

2.3 The Trust must ensure that each parent or carer of a child is notified of the Academy's intention to use the child's **biometric data** as part of an automated biometric recognition system.

2.4 The written consent of at least one parent or carer must be obtained before the data is taken from the child and used ie, **'processed'**. This applies to all students in schools and colleges **under the age of 18.** In no circumstances can a child's biometric data be processed without written consent.

2.5 Schools and colleges must not process the biometric data of a student (under 18 years of age) where:

a) The child (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data;

b) No parent/carer has consented in writing to the processing; or

c) A parent has objected in writing to such processing, even if another parent has given written consent.

2.6 Schools and colleges must provide reasonable alternative means of accessing services for those students who will not be using an automated biometric recognition system.

3. DEFINITIONS

3.1 *Biometric data* means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allows or confirms the unique identification of that natural person, such as facial images or finger print data. The Information Commissioner considers all biometric information to be sensitive personal data as defined by the **GDPR 2018**; this means that it must be obtained, used and stored in accordance with that Regulation. 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 **GDPR 2018**.

3.2 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 3.1 above.

3.3. '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.

4 CONSENT OF PARENTS AND CARERS

4.1 Any objection or consent by a parent or carer must be an informed decision – as should any objection on the part of a child. The Trust will take steps to ensure parents/carers 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 will be provided with information in a manner that is appropriate to their age and understanding. Each new system that is introduced will require separate consent.

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

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.

4.3 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.

5 CONSENT OF CHILD

A student 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 Trust will not collect or process the data where there is any doubt about the child's consent being given.

6 CONSULTATION ON THE USE OF AUTOMATED BIOMETRIC RECOGNITION SYSTEMS

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. The Trust may decide it is appropriate to consult parents and students in advance of introducing such a system for a number of practical reasons.

7 THE USE OF PHOTOGRAPHS AND CCTV

Consent is not needed the use of photographs and CCTV unless it is for the purposes of an automated biometric recognition system. However, the Trust must continue to comply with the requirements in the **GDPR 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 **GDPR 2018** before personal data is processed.

The Government believes that the GDPR 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 them 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.