



The Queen Katherine School Multi Academy Trust

PROTECTION OF BIOMETRIC INFORMATION POLICY

This policy does not form part of any employee's contract of employment and we may amend it from time to time.

Committee	MAT Board
Date of adoption:	October 2021
Date of next review	Annually

Document Control Sheet

The information in the table below details earlier versions of this document with a brief description of each review and how to distinguish amendments made since the previous version date (if any).

Version Number	Amended by	Purpose	Approved by Trustees (date)
I	THO	Original – based on latest DfE guidance March 2018. SJA Note: Checked DfE Jan 2022 and no subsequent updates.	Oct 2020

1. AIMS

Schools have a legal duty if they wish to use biometric information about students for the purposes of using automated biometric recognition systems. The duties on schools in the Protection of Freedoms Act 2012 set out in this advice came into effect from 1 September 2013.

Schools using automated biometric recognition systems, or planning to install them, should make arrangements to notify parents and obtain the consent required under the duties set out in the body of this advice. There are no circumstances in which a school or college can lawfully process a student's biometric data without having notified each parent of a child and received the necessary consent.

This advice relates to the following legislation:

- The Protection of Freedoms Act 2012
- The Data Protection Act 2018

2. KEY POINTS

- Schools 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 Data Protection Act 2018.
- Where the data is used as part of an automated biometric recognition system, schools must also comply with the additional requirements in sections 26 to 28 of the Protection of Freedoms Act 2012 (see relevant section below).
- Schools must ensure that each parent of a child is notified of the school's intention to use the child's biometric data as part of an automated biometric recognition system.
- 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 schools under the age of 18. In no circumstances can a child's biometric data be processed without written consent.
- Schools 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
 - a parent has objected in writing to such processing, even if another parent has given written consent
- Schools must provide reasonable alternative means of accessing services for those students who will not be using an automated biometric recognition system.

3. WHAT IS BIOMETRIC DATA?

- 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 dactyloscopic data.
- 3.2 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.
- 3.3 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.

4. WHAT IS AN AUTOMATED BIOMETRIC RECOGNITION SYSTEM?

- 4.1 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.
- 4.2 Biometric recognition systems can use many kinds of physical or behavioural characteristics such as those listed in 3.1 above.

5. WHAT DOES PROCESSING DATA MEAN?

'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
- 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.

6. THE PROTECTION OF FREEDOMS ACT 2012

6.1 Notification and Parental Consent

What the law says:

- a) Schools must notify each parent of a student under the age of 18 if they wish to take and subsequently use the child's biometric data as part of an automated biometric recognition system.
- b) As long as the child or a parent does not object, the written consent of only one parent will be required for a school or college to process the child's biometric information. A child does not have to object in writing but a parent's objection must be written.
- c) Schools will not need to notify a particular parent or seek his or her consent if the school is satisfied that:
 - the parent cannot be found, for example, his or her whereabouts or identity is not known
 - the parent lacks the mental capacity to object or to consent
 - the welfare of the child requires that a 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
 - where it is otherwise not reasonably practicable for a particular parent to be notified or for his or her consent to be obtained.
- d) Where neither 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 either of them), section 27 of the Protection of Freedoms Act 2012 sets out who should, in such circumstances, be notified and who can give consent:
 - if the child is being 'looked after' by a local authority or is accommodated or maintained by a voluntary organisation (i.e. a not-for-profit organisation), the local authority, or as the case may be, the voluntary organisation must be notified and their written consent obtained.
 - if the bullet point above does not apply, then notification must be sent to all those caring for the child and written consent must be gained from at least one carer before the child's biometric data can be processed (subject to the child and none of the carers objecting in writing).

- e) There will never be any circumstances in which a school or college can lawfully process a child's biometric information (for the purposes of using an automated biometric recognition system) without one of the persons above having given written consent.
- f) 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 should have contact details for most parents in the admission register.
- g) Schools should 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, the school might ask 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, may make enquiries with the local authority or other agency. Schools and colleges are not expected to engage the services of 'people tracer' or detective agencies but are expected to take reasonable steps to locate a parent before they are able to rely on the exemption in section 27(1)(a) of the Protection of Freedoms Act (i.e. notification of a parent not required if the parent cannot be found).
- h) An option would be for schools to notify parents that they intend to take and use their child's biometric information as part of an automated biometric recognition system and seek written consent to do so at the same time as obtaining details of parents as part of the enrolment process. In other words, details of both parents would be requested by the school or college for both purposes (enrolment and notification of intention to process biometric information).
- i) Notification sent to parents should include information about the processing of their child's biometric information that is sufficient to ensure that parents are fully informed about what is being proposed. This should include: details about the type of biometric information to be taken; how it will be used; the parents' and the student's right to refuse or withdraw their consent; and the school's duty to provide reasonable alternative arrangements for those pupils whose information cannot be processed.

6.2 The Student's Right to Refuse

What the law says:

- a) If a student under 18 objects or refuses to participate (or to continue to participate) in activities that involve the processing of their biometric data, the school must ensure that the student's biometric data is not taken/used as part of a biometric recognition system. A student's objection or refusal overrides any parental consent to the processing.
- b) Schools should take steps to ensure that students understand that they can object or refuse to allow their biometric data to be taken/used and that, if they do this, the school will have to provide them with an alternative method of accessing relevant services. The steps taken by schools to inform students should take account of their age and level of understanding. Parents should also be told of their child's right to object or refuse and be encouraged to discuss this with their child.
- c) In addition to the required actions for notification and obtaining consent, schools may wish to include information in their privacy notices and explain how biometric data is to be processed and stored by the school.

6.3 Providing Alternatives

What the law says:

- a) Reasonable alternative arrangements must be provided for students who do not use automated biometric recognition systems either because their parents have refused consent (or a parent has objected in writing) or due to the student's own refusal to participate in the collection of their biometric data.
- b) The alternative arrangements should ensure that students do not suffer any disadvantage or difficulty in accessing services/premises etc. because of their not participating in an automated

biometric recognition system. Likewise, such arrangements should not place any additional burden on parents whose children are not participating in such a system.