Protection of Biometric Information Policy

Prepared by:	Barbara Smith
Date:	September 2020
Review date:	July 2021
Approved by:	Trust Board 28th September 2020
Trustee Minute No:	0145.5

Live

Contents

1.0 Statement of intent

QEGSMAT (the Trust) is committed to protecting the personal data of all its students, pupils and staff, this includes any biometric data we collect and process.

We collect and process biometric data in accordance with relevant legislation and guidance to ensure the data and rights of individuals are protected. This policy outlines the procedure the Trust follows when collecting and processing biometric data.

2.0 Definitions

Biometric data: Personal information about an individual's physical or behavioural characteristics that can be used to identify that person, including their fingerprints, facial shape, retina and iris patterns, and hand measurements.

Automated biometric recognition system: A system 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.

Processing biometric data: Processing biometric data includes obtaining, recording or holding the data or carrying out any operation on the data including disclosing it, deleting it, organising it or altering it. An automated biometric recognition system processes data when:

- Recording pupil/student biometric data, e.g. taking measurements from a fingerprint via a fingerprint scanner.
- Storing pupil/student biometric information on a database.
- Using pupil/student biometric data as part of an electronic process, e.g. by comparing it with biometric information stored on a database to identify or recognise pupils/students.

Special category data: Personal data which the GDPR says is more sensitive, and so needs more protection – where biometric data is used for identification purposes, it is considered special category data.

3.0 Roles and responsibilities

The Trust is responsible for:

- Reviewing this policy on an annual basis.

The Headteacher is responsible for:

- Ensuring the provisions in this policy are implemented consistently.

The Data Protection Officer (DPO) is responsible for:

- Monitoring the school's compliance with data protection legislation in relation to the use of biometric data.
- Advising on when it is necessary to undertake a data protection impact assessment (DPIA) in relation to the school's biometric system(s).

- Being the first point of contact for the ICO and for individuals whose data is processed by the school and connected third parties.

4.0 Data protection principles

4.1 The Trust processes all personal data, including biometric data, in accordance with the key principles set out in the GDPR.

4.2 The Trust ensures biometric data is:

- Processed lawfully, fairly and in a transparent manner.
- Only collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date, and that reasonable steps are taken to ensure inaccurate information is rectified or erased.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Processed in a manner that ensures appropriate security of the information, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4.3 As the data controller, the Trust is responsible for being able to demonstrate its compliance with the provisions outlined in 4.2.

5.0 Data protection impact assessments

5.1 Prior to processing biometric data or implementing a system that involves processing biometric data, a DPIA will be carried out.

5.2 The DPO will oversee and monitor the process of carrying out the DPIA.

5.3 The DPIA will:

- Describe the nature, scope, context and purposes of the processing.
- Assess necessity, proportionality and compliance measures.
- Identify and assess risks to individuals.
- Identify any additional measures to mitigate those risks.

5.4 When assessing levels of risk, the likelihood and the severity of any impact on individuals will be considered.

5.5 If a high risk is identified that cannot be mitigated, the DPO will consult the ICO before the processing of the biometric data begins.

5.6 The ICO will provide the school with a written response (within eight weeks or 14 weeks in complex cases) advising whether the risks are acceptable, or whether the school needs to take further action. In some cases, the ICO may advise the school to not carry out the processing.

5.7 The school will adhere to any advice from the ICO.

6.0 Notification and consent

Please note that the obligation to obtain consent for the processing of biometric information of children under the age of 18 is not imposed by the Data Protection Act 2018 or the GDPR. Instead, the consent requirements for biometric information is imposed by section 26 of the Protection of Freedoms Act 2012.

6.1 Where the school uses pupil/students' biometric data as part of an automated biometric recognition system (e.g. using fingerprints to receive school dinners instead of paying with cash), the school will comply with the requirements of the Protection of Freedoms Act 2012.

6.2 Prior to any biometric recognition system being put in place or processing a pupil/student's biometric data, the school will send the pupil/student's parents/carer a Parental Notification and Consent Form for the use of Biometric Data.

6.3 Written consent will be sought from at least one parent/carer of the pupil/student before the school collects or uses biometric data.

6.4 The name and contact details of the pupil/student's parents/carers will be taken from the school's admission register.

6.5 Where the name of only one parent/carer is included on the admissions register, the headteacher will consider whether any reasonable steps can or should be taken to ascertain the details of the other parent/carer.

6.6 The school does not need to notify a particular parent/carer or seek their consent if it is satisfied that:

- The parent/carer cannot be found, e.g. their whereabouts or identity is not known.
- The parent/carer lacks the mental capacity to object or consent.

- The welfare of the pupil/student requires that a particular parent/carer is not contacted, e.g. where a pupil/student has been separated from an abusive parent/carer who must not be informed of the child's whereabouts.
- It is otherwise not reasonably practicable for a particular parent/carer to be notified or for their consent to be obtained.

6.7 Where neither parent/carer of a pupil/student can be notified for any of the reasons set out in 6.6, consent will be sought from the following individuals or agencies as appropriate:

- If a pupil/student is being 'looked after' by the Local Authority (LA) or is accommodated or maintained by a voluntary organisation, the LA or voluntary organisation will be notified and their written consent obtained.
- If the above does not apply, then notification will be sent to all those caring for the pupil/student and written consent will be obtained from at least one carer before the biometric data can be processed.

6.8 Notification sent to parents/carers and other appropriate individuals or agencies will include information regarding the following:

- Details about the type of biometric information to be taken
- How the data will be used.
- The parent's and the pupil's right to refuse or withdraw their consent.
- The school's duty to provide reasonable alternative arrangements for those pupils whose information cannot be processed.

6.9 The school will not process the biometric data of a pupil/student under the age of 18 in the following circumstances:

- The pupil/student (verbally or non-verbally) objects or refuses to participate in the processing of their biometric data.
- No parent or carer has consented in writing to the processing.
- A parent/carer has objected in writing to such processing, even if another parent/carer has given written consent.

6.10 Parents/carers and pupils/students can object to participation in the school's biometric system(s) or withdraw their consent at any time. Where this happens, any biometric data relating to the pupil/student that has already been captured will be deleted.

6.11 If a pupil/student objects or refuses to participate, or to continue to participate, in activities that involve the processing of their biometric data, the school will ensure that the biometric data is not taken or used as part of a

biometric recognition system, irrespective of any consent given by the parent/carer(s).

6.12 Pupils/students will be informed that they can object or refuse to allow their biometric data to be collected and used via a letter.

6.13 Where staff members or other adults use the school's biometric system(s), consent will be obtained from them before they use the system.

6.14 Staff and other adults can object to taking part in the school's biometric system(s) and can withdraw their consent at any time. Where this happens, any biometric data relating to the individual that has already been captured will be deleted.

6.15 Alternative arrangements will be provided to any individual who does not consent to take part in the school's biometric system(s), in line with Section 7 of this policy.

7.0 Alternative arrangements

7.1 Parents, carers, students, pupils, staff members and other relevant adults have the right to not take part in the school's biometric system(s).

7.2 Where an individual objects to taking part in the school's biometric system(s), reasonable alternative arrangements will be provided that allow the individual to access the relevant service, e.g. issuing the individual with a Personal Identification Number (PIN) or using their school ID card. The exact method will vary depending on the capability of the school/service providers systems.

7.3 Alternative arrangements will not put the individual at any disadvantage or create difficulty in accessing the relevant service, or result in any additional burden being placed on the individual (and the pupil/student's parents/carers, where relevant).

8.0 Data retention

8.1 Biometric data will be managed and retained in line with the Trust's Data Protection policy.

8.2 If an individual (or a pupil's/student's parent/carer, where relevant) withdraws their consent for their/their child's biometric data to be processed, it will be erased from the school's system.

9.0 Breaches

9.1 There are appropriate and robust security measures in place to protect the biometric data held by the school. These measures are detailed in the Trust's Data Protection policy.

9.2 Any breach to the school's biometric system(s) will be dealt with in accordance with the Data Protection policy.

Appendix 1 – Parental consent form for use of biometric data

BIOMETRIC SYSTEM

We operate a biometric cashless system in school that avoids the need for students to pay cash for their meals. The system uses the latest biometric technology that is able to recognise the thumb or finger of the student at the revaluation pay points and at the tills.

The cashless solution does not store finger prints. When a finger is originally scanned the system creates a unique algorithm from the scanned points. This data is then immediately encrypted and as such serves no purpose other than unique identification within the school.

Do you give permission for your child to use the biometric system and have their thumb/finger print scanned?

You understand that if they don't use this system, students will be allocated a PIN instead, for which they are responsible for remembering and keeping secure.

Do you give permission for your child to use the biometric system and have their thumb/finger print scanned?

Yes (I agree to this) | No (I do not agree to this)
(Delete as applicable)

Signature: _____

Name: _____

Date: _____