Testbourne Community School

TCS Protection of Children's Biometric Information Policy

Review cycle:	Annually
Policy prepared / reviewed by:	J Worth
Committee responsible:	Finance, Business and Community
Statutory/Discretionary:	Statutory
Date of last review:	02/02/2021
Date of next review:	02/02/2022
Approval Cycle	Spring Term

Contents

1. Key Points

- Testbourne Community School (henceforth referred to as 'the school') uses students' biometric data (see 1 below) and will treat the data collected with appropriate care and will comply with the data protection principles as set out in the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA 2018).
- Where the data is used as part of an automated biometric recognition system (see 2 below), the school will comply with the additional requirements in sections 26 to 28 of the Protection of Freedoms Act 2012 (see relevant section below).
- The school will ensure that each parent of a child is notified of the school's intention to use the child's biometric data (see 1 below) 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' – see 3 below). This applies to all students under the age of 13. In no circumstances can a student's biometric data be processed without written consent.
- Students over the age of 13 years of age can consent themselves.
- The school will not process the biometric data of a pupil (under 13 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 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.
- The school will provide reasonable alternative means of accessing services for those pupils who will not be using an automated biometric recognition system.

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 fingerprints, facial shape, retina and iris patterns, and hand measurements.
- The Information Commissioner considers all biometric information to be personal data as defined by the DPA 2018; this means that it must be obtained, used and stored in accordance with that Act (see relevant paragraphs below).
- The Protection of Freedoms Act 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 DPA 2018. (See relevant section below).

What is an automated biometric recognition system?

- An automated biometric recognition system uses technology which measures an individual's physical or behavioural characteristics[1] 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 section 1 of the 'What is biometric data' section above.

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[2]. An automated biometric recognition system processes data when:

1.
    a. recording students' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner;

    b. storing students' biometric information on a database system; or

    c. 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.
2. More information on these topics is available via the **Associated Resources** section below.

2. The Protection of Freedoms Act 2012

Notification and Parental Consent

What the law says:

1) Schools and colleges must notify each parent[3] of a student under the age of 13 if they wish to take and subsequently use the child's biometric data as part of an automated biometric recognition system.

2) Provided 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, if

[1] Biometric systems usually store measurements taken from a person's physical/behavioural characteristics and not images of the characteristics themselves. For example, a fingerprint image is not stored on the system but measurements from the fingerprint are converted into a template and the template is stored. The templates are also biometric data.

[2] See section 1(1) of the Data Protection Act 2018.

[3] The parents of a child include not only the biological mother or father (or the adoptive parents) but any other individual with parental responsibility for the child. Part 1 of the Children Act 1989 sets out who has parental responsibility and what this means.

the child is under the age of 13. A child under the age of 13 does not have to object in writing but a parent's objection must be written.

3) Schools and colleges will not need to notify a parent or seek his or her consent if the school or college is satisfied that:

   a. the parent cannot be found, for example, his or her whereabouts or identity is not known;

   b. the parent lacks the mental capacity[4] to object or to consent;

   c. the welfare of the child requires that a 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; or

   d. where it is otherwise not reasonably practicable for a parent to be notified or for his or her consent to be obtained.

4) 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:

   a. if the child is being 'looked after' by a local authority[5] 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.

   b. if paragraph (a) 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).

5) 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.

6) 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.

7) 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

[4] Within the meaning of the Mental Capacity Act 2005.

[5] For example, the child is subject to a care order in favour of the local authority or the local authority provides accommodation for the child – see section 22 of the Children Act 1989 for the definition of 'looked after' child.

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).

8) An option would be for schools and colleges 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).

9) 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 pupil'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.

The pupil's right to refuse

What the law says:

1) If a student under the age of 13 objects or refuses to participate (or to continue to participate) in activities that involve the processing of their biometric data, the school or college must ensure that the pupil's biometric data are not taken/used as part of a biometric recognition system. A pupil's objection or refusal overrides any parental consent to the processing.

Also note:

2) Schools and colleges 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 or college will have to provide them with an alternative method of accessing relevant services. The steps taken by schools and colleges 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.

3) In addition to the required actions for notification and obtaining consent, the school uses its Privacy Notices to further explain how biometric data is processed and stored by the school.

Providing alternatives

What the law says:

1) 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.

2) The alternative arrangements should ensure that pupils do not suffer any disadvantage or difficulty in accessing services/premises etc. as a result 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.

The Data Protection Act 2018

1) As *data controllers*, the school will process students' *personal data* (which includes biometric data), in accordance with the GDPR and DPA 2018. The provisions in the Protection of Freedoms Act 2012 are in addition to the requirements under the DPA 2018 with which schools and colleges must continue to comply.

2) The DPA 2018 has six data protection principles with which all data controllers must comply.

3) When processing a student's personal data, including biometric data for the purposes of an automated biometric recognition system, schools and colleges must comply with these principles. This means, for example, that they are required to:

    a. Store biometric data securely to prevent any unauthorised or unlawful use.

    b. Not keep biometric data for longer than it is needed meaning that a school or college must destroy a child's biometric data if, for whatever reason, the child no longer uses the system including when he or she leaves the school or college or where a parent withdraws consent or the child objects.

    c. Ensure that biometric data is used only for the purposes for which they are obtained and that such data are not unlawfully disclosed to third parties.

For more information about the data protection principles and practical advice, see the **Associated Resources** section below.

Associated Resources

- DfE guidelines for schools on communicating with parents and obtaining consent:
- https://www.gov.uk/government/publications/dealing-with-issues-relating-toparental-responsibility.

- ICO guide to data protection: http://www.ico.gov.uk/for_organisations/data_protection/the_guide.aspx.

- ICO guidance on data protection for education establishments: http://www.ico.gov.uk/for_organisations/sector_guides/education.aspx.

- British Standards Institute guide to biometrics: Biometrics Website for news updates standards - biometric systems - BSI Shop

3. Notification of Intention to Process Students' Biometric Information

Testbourne Community School (henceforth referred to as 'the school') wishes to use information about your child as part of an automated (i.e. electronically operated) recognition system. This is for the purposes of Cashless Catering. The information from your child that we wish to use is referred to as 'biometric information' (see next paragraph). Under the Protection of Freedoms Act 2012 (sections 26 to 28), we are required to notify each parent of a child and obtain the written consent of at least one parent before being able to use a child's biometric information for an automated system.

Biometric information and how it will be used

Biometric information is information about a person's physical or behavioural characteristics that can be used to identify them, for example, information from their fingerprint. The school would like to take and use information from your child's fingerprint and use this information for the purpose of providing your child with automated recognition for their Cashless Catering account.

The information will be used as part of an automated biometric recognition system. This system will take measurements of your child's fingerprint and convert these measurements into a template to be stored on the system. An image of your child's fingerprint is not stored. The template (i.e. measurements taking from your child's fingerprint) is what will be used to permit your child to access this service.

You should note that the law places specific requirements on the school when using personal information, such as biometric information, about pupils for the purposes of an automated biometric recognition system.

For example:

(a) the school cannot use the information for any purpose other than those for which it was originally obtained and made known to the parent(s) (i.e. as stated above);

(b) the school must ensure that the information is stored securely;

(c) the school must tell you what it intends to do with the information;

(d) unless the law allows it, the school cannot disclose personal information to another person/body – you should note that the only person/body that the school wishes to share the information with is CRB Cunninghams and BioStore as the system suppliers. This is necessary in order to ensure efficient and secure running of the system as well as to carry out any troubleshooting.

Providing your consent/objecting

As stated above, in order to be able to use your child's biometric information, the written consent of at least one parent is required. However, consent given by one parent will be overridden if the other parent objects in writing to the use of their child's biometric information. Similarly, if your child objects to this, the school cannot collect or use his/her biometric information for inclusion on the automated recognition system.

You can also object to the proposed processing of your child's biometric information at a later stage or withdraw any consent you have previously given. This means that, if you give

consent but later change your mind, you can withdraw this consent. Please note that any consent, withdrawal of consent or objection from a parent must be in writing.

Even if you have consented, your child can object or refuse at any time to their biometric information being taken/used. Their objection does not need to be in writing. We would appreciate it if you could discuss this with your child and explain to them that they can object to this if they wish.

The school is also happy to answer any questions you or your child may have.

If you do not wish your child's biometric information to be processed by the school, or your child objects to such processing, the law says that we must provide reasonable alternative arrangements for children who are not going to use the automated system for Cashless Catering.

If you give consent to the processing of your child's biometric information, please sign, date and return the enclosed consent form to the school.

Please note that when your child leaves the school, or if for some other reason he/she ceases to use the biometric system, his/her biometric data will be securely deleted.

Further information and guidance

This can be found via the following links:

Department for Education's *'Protection of Biometric Information of Children in Schools – Advice for proprietors, governing bodies, head teachers, principals and school staff'*: http://www.education.gov.uk/schools/adminandfinance/schooladmin.

ICO guide to data protection for organisations: Guide to data protection | ICO

ICO guidance on data protection for education establishments: Education | ICO.

4. Consent Form for Parents

Biometrics Testbourne operates a “cashless catering” system. Essentially this means that there are no cash transactions in the Dining Room. Parents can pay in the sums they choose on-line directly into their child’s account, in the same way that parents do for school trips using the “payments to school” link on the school website.

The benefits of the cashless system include students needing to carry less cash on them; increased parental control of how students spend their lunch money; free school meals automatically and discreetly included; and a faster service in the Canteen. We collect biometric fingerprints from students in order to register them to use the system and any other system requiring a student’s identification via biometrics.

Students and parents can be rest assured that the fingerprint images cannot be used by any other source for identification purposes. The system uses an image of the fingerprint to create a mathematical algorithm and this discards the fingerprint; only the algorithm numbers remain and these cannot be reinterpreted back into a fingerprint image.

All the data will be handled under the guidelines of the General Data Protection Regulation (GDPR) and only used by parties directly involved with the implementation of the system.

If you do not consent to your child’s fingerprint being registered on the system, an alternative method of identification will be made available.

If at any point you wish to withdraw consent for the use of your child’s fingerprint, please do this in writing to your child’s tutor. The tutor will then pass this on to the school’s Data Protection Officer who will confirm deletion within 5 working days.

Child’s Name:

I consent to my child’s fingerprint being registered on the system:

Yes ☐

No ☐

Parent/Carer Name:

Signature: **Date:**