

# Trinity Catholic High School



## Biometric Data Guidance

**Approved by:** Governors **Date:** 12 July 2023

**Last reviewed on:** June 2023

**Next review due by:** June 2024

1. What is biometric data?.....	3
2. What is an automated biometric recognition system? .....	3
3. What does processing data mean?.....	3
4. The Protection of Freedoms Act 2012 .....	4
5. The UK General Data Protection Regulations (UK GDPR) and Data Protection Act 2018 (DPA).....	7
6. Appendix A.....	8

## **1. 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 UK General Data Protection Regulations (UK GDPR) and Data Protection Act 2018 (DPA); this means that it must be obtained, used and stored in accordance with these requirements (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 UK GDPR and DPA. (See relevant section below).

## **2. What is an automated biometric recognition system?**

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 section 1 of the 'What is biometric data' section above.

## **3. What does processing data mean?**

The term 'Processing' is defined under the UK GDPR and DPA as any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

An automated biometric recognition system processes data when:

- a. recording pupils' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner;
- b. storing pupils' 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 pupils.

#### 4. The Protection of Freedoms Act 2012

**Notification and Parental Consent (Where the data are to be used as part of an automated Biometric recognition system)** (see 2 above), schools and colleges must also comply with the additional requirements in sections 26 to 28 of the **Protection of Freedoms Act 2012.**)

The written consent of at least one parent must be obtained before the data are taken from the child and used (i.e. **'processed'** – see 3 above). This applies to all pupils in schools and colleges **under the age of 18**. In no circumstances can a child's biometric data be processed without written consent.

*What the law says:*

- 1) Schools and colleges must notify each parent of a pupil 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.
- 2) 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.
- 3) Schools and colleges will not need to notify a particular 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 to object or to consent;
  - c. 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; or
  - d. where it is otherwise not reasonably practicable for a particular 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 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 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 pupil under 18 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.

2) Schools and colleges should take steps to ensure that pupils 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 pupils 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, schools and colleges may wish to include information in their privacy notices and explain how biometric data is to be processed and stored by the school.

### **Providing alternatives**

*What the law says:*

1) Reasonable alternative arrangements must be provided for pupils 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 pupil'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.

## **5. The UK General Data Protection Regulations (UK GDPR) and Data Protection Act 2018 (DPA)**

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

The UK GDPR and DPA has six data protection principles with which all data controllers must comply.

When processing a pupil'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.

### **Special Category data**

Schools must still have a lawful basis for processing under Article 6, in exactly the same way as for any other personal data. The difference is that we will also need to satisfy a specific condition under Article 9.

This is because special category data is more sensitive, and so needs more protection. Biometric data is considered to be special category data.

The schools choice of lawful basis under Article 6 does not dictate which special category condition must be applied, and vice versa. For example, if we use consent as our lawful basis, we are not restricted to using explicit consent for special category processing under Article 9.

## 6. Appendix A

### Template Notification and Consent

The following is suggested text for a notification letter and consent form for schools and colleges to use to notify parents of their plans to collect and use biometric data. Schools and colleges may wish to adapt this text in light of their own particular systems but should ensure that parents are made aware of the school's and college's requirements as set out in sections 26-28 of the Protection of Freedoms Act 2012.

#### **NOTIFICATION OF INTENTION TO PROCESS PUPILS' BIOMETRIC INFORMATION**

**Dear [*name of parent/carer*]**

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 catering, and in some cases registration. 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 fingerprints. Trinity Catholic High 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 school meals instead of paying using cash and in some cases fingerprints will be used for registration purposes.

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 taken from your child's fingerprint) is what will be used to permit your child to access services.

You should note that the law places specific requirements on schools and colleges 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 Cunningham's and Joskos. This is necessary in order to provide support and access to the services.

### **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. [*His/her*] 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 to pay for school meals and to register.

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

**For a copy of the consent form(s) please refer to the Data Protection Policy.**