STCAT PROTECTION OF BIOMETRIC DATA POLICY

Author	**Maxine Gilmartin**
Date	**January 2022**
Version	**1.0**
Date approved by Board	**24 January 2022**
Review date	**January 2024**

Contents

1. Aims

St Thomas Catholic Academies Trust (the "Trust") is committed to protecting the personal data of all its pupils and staff, this includes any biometric data we collect and process.

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

2. Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Protection of Freedoms Act 2012
- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- DfE (2018) 'Protection of biometric information of children in schools and colleges'

This policy operates in conjunction with the following Trust policies:

- STCAT Data Protection Policy
- STCAT Data Retention Schedule

3. Definitions

Term	Definition
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. Within the Trust, we use fingerprints only.
Automated biometric recognition system	A system which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (ie 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 pupils' biometric data, eg taking measurements from a fingerprint via a fingerprint scanner. • Storing pupils' biometric information on a

	database. • Using pupils' biometric data as part of an electronic process, eg by comparing it with biometric information stored on a database to identify or recognise pupils.
Special category data	Personal data which the UK GDPR says is more sensitive, and so needs more protection – where biometric data is used for identification purposes, it is considered special category data.
Information Commissioner's Officer (ICO)	The UK data protection regulator.

4. Roles and Responsibilities

4.1 The Trust Board is responsible for reviewing this policy on a biennial basis.

4.2 The Headteacher of each school is responsible for ensuring the provisions in this policy are implemented consistently.

4.3 The Data Protection Lead (DPL) in each school is responsible for:

- Monitoring the school's compliance with data protection legislation in relation to the use of biometric data.

4.4 The Trust's Data Protection Officer

- Advising on when it is necessary to undertake a data protection impact assessment (DPIA) in relation to the Trust's biometric system(s).
- Being the first point of contact for the ICO and for individuals whose data is processed by schools and connected third parties.

5. Data protection principles

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

5.2 The Trust ensure biometric data is:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

5.3 As the Data Controller, the Trust is responsible for being able to demonstrate its compliance with the provisions outlined at 5.2. The UK GDPR principles are detailed further in the Trust Data Protection Policy. The Trust DPO can be contacted at admin@stcat.co.uk.

6. Data protection impact assessments (DPIA)

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

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

6.3 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.

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

6.5 If a high risk is identified that cannot be mitigated, the DPO will consult the ICO before the processing of the biometric data begins. The ICO will provide the DPO with a written response (within eight weeks or 14 weeks for complex cases) advising whether the risks are acceptable, or whether the Trust needs to take further action. In some cases, the ICO may advise the Trust to not carry out the processing. The Trust will adhere to any advice from the ICO.

7. Notification and consent

7.1 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 UK GDPR. Instead, the consent requirements for biometric information is imposed by section 26 of the Protection of Freedoms Act 2012.

7.2 Where a school uses pupils' biometric data as part of an automated biometric recognition system (eg for school dinners instead of paying with cash or a PIN), the school will comply with the requirements of the Protection of Freedoms Act 2012.

7.3 Prior to processing a pupil's biometric data, the school will send the parents/carers a consent form or collect this consent via secure online systems.

7.4 Consent will be sought from at least one parent/carer of the pupil before the school collects or uses a pupil's biometric data.

7.5 Information provided to parents/carers will include information regarding the following:

- How the data will be used.
- The parent/carer and the child'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.

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

- The pupil (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 has objected in writing to such processing, even if another parent has given written consent.

7.7 Parents/carers and pupils 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 that has already been captured will be deleted.

7.8 If a pupil objects or refuses to participate, or to continue to participate, in activities that involve the processing of their biometric data, the school will ensure the pupil's biometric data is not taken or used as part of a biometric recognition system, irrespective of any consent given by the pupil's parent/carer.

7.9 Pupils will be informed that they can object or refuse to allow their biometric data to be collected and used via the consent information.

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

7.11 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.

7.12 Alternative arrangements will be provided to any individual that does not consent to take part in a school's biometric system(s), in line with Section 8 of this policy.

8. Alternative arrangements

8.1 Pupils and staff have the right to not take part in the school's biometric system.

8.2 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, eg where a biometric system uses fingerprints to pay for school meals, the person may be able to use a 4 digit PIN instead or by name lookup.

8.3 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's parents/carers, where relevant).

9. Data retention

9.1 Biometric data will be managed and retained in line with the Trust's Data Retention Schedule.

9.2 If an individual (or a pupil'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.

10. Breaches

10.1 There are appropriate and robust security measures in place to protect the biometric data held by the school.

10.2 Any breach to the school's biometric system will be dealt with by the Trust DPO.

Appendix 1: Biometric consent form (parent/carer)

Please sign below if you consent to the school taking and using information from your son/daughter's fingerprint as part of an automated biometric recognition system. This biometric information will be used by the school for the purposes of administration of school meals.

In signing this form, you are authorising the school to use your son/daughter's biometric information for this purpose until he/she either leaves the school or ceases to use the system.

If you wish to withdraw your consent at any time, this must be done so in writing and sent to the Headteacher. Once your son/daughter ceases to use the biometric recognition system, his/her biometric information will be securely deleted.

Parent/Carer consent:

Having read the above guidance information, I give consent to information from the fingerprint of my son/daughter being taken and used by the school for use as part of an automated biometric recognition system.

I understand that I can withdraw this consent at any time in writing.

Parent/Carer name:	
Signature:	
Date:	
Name of student:	
Class:	

Appendix 2: Biometric consent form (staff)

Please sign below if you consent to the school taking and using your fingerprint as part of an automated biometric recognition system. This biometric information will be used by the school for the purposes of administration and supply of food and meals through the school's catering provider.

In signing this form, you are authorising the school to use your biometric information for this purpose until you either leave the school or ceases to use the system.

If you wish to withdraw your consent at any time, this must be done so in writing and sent to the Headteacher.

Having read the above guidance information, I give consent to information from my fingerprint being taken and used by the school for use as part of an automated biometric recognition system.

I understand that I can withdraw this consent at any time in writing.

Staff name:	
Signature:	
Date:	

Appendix 3: Template notification letter

NOTIFICATION OF INTENTION TO PROCESS PUPILS' BIOMETRIC INFORMATION

Dear [ ]

The school wishes to use information about your child as part of an automated (ie electronically operated) recognition system. This is for the purposes of [*specify what purposes is*]. The information from your child that we wish to use is referred to as 'biometric information'. Under the Protection of Freedoms Act 2012 (sections 26-28), 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 [*insert biometric to be used*] and use this information for the purpose of providing your child with [*specify what purpose is*].

The information will be used as part of an automated biometric recognition system. This system will take measurements of your child's [*insert biometric to be used*] and convert these measurements into a template to be stored on the system. An image of your child's [*insert biometric*] is <u>not</u> stored. The template (ie measurements taken from your child's [*insert biometric*]) is what will be used to permit your child to access services.

You should note that the law places specific requirements on schools 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) (ie 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 [*insert any third party with which the information is to be shared, eg X supplier of biometric systems*]. This is necessary in order to [*say why it needs to be disclosed to the third party*].

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 [*insert relevant service*].

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

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.