St Ralph Sherwin
Catholic Multi Academy Trust

Protection of Biometric Information Policy

Version 1
March 2022

One of four Catholic Multi Academy Trusts in the Diocese of Nottingham

Document Provenance

Title of policy:	Protection of Biometric Information Policy	
Author and policy owner in the Executive Team:	Head of Governance / DPO - reporting to the CEO.	
Version number:	1	
Date approved:	8 March 2022	
Approved by:	Finance and Estates Committee	
Date of next review:	March 2023	
Document review and editorial updates:		
Version control	**Date**	**Key revisions included**
1	2 March 2022	This is a brand new policy to be used by all Academies within the Trust. It sets out the required procedures and expectations in using biometric data and how through this policy the Trust ensures full compliance with required legislation.

Saint Ralph Sherwin Catholic Multi Academy Trust Vision

Academies within The Saint Ralph Sherwin Catholic Multi Academy Trust ensure that each child is treated individually and with respect. We lead by the example of our namesake, Saint Ralph Sherwin, a martyr who risked all for his faith, seeking to do the Lord's will "today rather than tomorrow". All academies within the Saint Ralph Sherwin Catholic Multi Academy Trust share the same collective vision:

Vision

We are a Catholic family of schools, working as one, transforming every individual, their family and our Trust community through the building of God's Kingdom, caring for our environment, today rather than tomorrow.

Our Mission

'Inspired by the life, message and example of Jesus Christ'

Our Core Values

Community

Being and building a Catholic family of schools working alongside the parents, parishes and communities we serve

Aspiration

Enabling the transformation of every pupil, employee and volunteer, across our Trust family so that all can be their best and do their best to transform our world for the benefit of all

Renewal

Building God's Kingdom here on earth every day in all that we do and say

Encounter

Encountering Jesus and helping all to grow in their relationship with him, today rather than tomorrow

Please follow the link below for further information regarding the St Ralph Sherwin Catholic Multi Academy Trust.

Our Vision and Values | St Ralph Sherwin Catholic Multi Academy Trust (srscmat.co.uk)

1. Introduction and Purpose

1.1. St Ralph Sherwin Catholic Multi Academy Trust is committed to protecting the personal data of all its pupils and staff, this includes any biometric data we collect and process.

1.2. As a Trust we fully adhere to the requirements that any Academy using or planning to use/install automated biometric recognition systems must make full and proper arrangements for notifying parents and obtaining the consent required under the Duties set out in this Policy. There are no circumstances in which an Academy can lawfully process a pupil's biometric data without having notified each parent of a child and received the necessary consent.

1.3. This policy supports our Trust in our collection and processing of biometric data in accordance with relevant legislation and guidance. This ensures that the data and the rights of individuals are protected. This policy sets out the procedures the Trust follows when collecting and processing biometric data.

2. Objectives

2.1. The objectives of this policy are to ensure that:

- The handling of all biometric data is fully compliant with all relevant legislation and guidance and reduces risk of any mishandling or data breach in its usage
- Pupils, their parents and staff are confident and assured that robust processes are in place for handling biometric data
- Across the Trust both at Academy level and in Trust central teams, everyone understands the processes and requirements in use of biometric data prescribed in this policy.

3. Scope

3.1. This policy applies to pupils and staff across the Trust.

4. Legislation and Regulation

4.1. This policy is written in accordance with and has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Protection of Freedoms Act 2012[1]
- Data Protection Act 2018[2]
- General Data Protection Regulation (GDPR)[3]
- DfE (2018) 'Protection of biometric information of children in schools and colleges' [4]

[1] Protection of Freedoms Act 2012 (legislation.gov.uk)
[2] Data Protection Act 2018 (legislation.gov.uk)
[3] Guide to the General Data Protection Regulation - GOV.UK (www.gov.uk)
[4] Protection of children's biometric information in schools - GOV.UK (www.gov.uk)

4.2. This policy must be read in conjunction with the following Trust policies as published on the Trust website:

- The Data Protection Policy
- The Information and Records Retention Policy

5. Definitions – Biometric Data

5.1. What is biometric data?

- Biometric data is 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.

5.2. What is an Automated Biometric Recognition System?

- This is a system which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (i.e., electronically). For example, this may include biometric recognition systems for:
  - Registration
  - The library
  - Purchasing food in the canteen
- 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.
- In using an Automated Biometric Recognition System Academies have to not only comply with the GDPR Regulations 2018 but also with the additional requirements set out in Sections 26-28 of the Protection of Freedoms Act 2012.

5.3. How do we process Biometric Data?

- The processing of 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/staff biometric data, e.g., taking measurements from a fingerprint via a fingerprint scanner.
  - Storing pupils/staff biometric information on a database.
  - Using pupils/staff 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.

5.4. What is Special Category Data?

- Special category data[1] is 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.

[1] Special category data | ICO

6. Data Protection Principles

6.1. The processing of all personal data, including biometric data, is in accordance with the key principles set out in GDPR

6.2.The Trust will ensure that biometric data is:

- Only collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes
- Processed lawfully, fairly and in a transparent manner
- 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.

6.3. The Trust is the Data Controller and the Trust is therefore responsible for being able to show it full compliance with the provisions outlined above.

7. Data Retention

7.1. The Trust will ensure that biometric data will be used, managed and retained in accordance with all of the requirements set out in the Information Records and Retention Policy.

7.2. If an individual (or a pupils' parent where relevant) withdraw their consent for their or their child's biometric data to be processed, the data will be erased from the Trust/Academy system. A record of the erasure of the data will be date and time stamped.

7.3. Where staff members or other adults use the Trust`s biometric system(s), consent will be obtained from them before they use the system.

7.4. Staff and other adults may choose to object to taking part in the Trust'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. At deletion there will be date and time stamped record of deletion.

8. Data Privacy Impact Assessments (DPIAs)

8.1. Before processing biometric data or implementing a system/s that involve processing biometric data, a Data Privacy Impact Assessment (DPIA) will be actioned.

8.2. The Data Protection Officer (DPO) working with the GDPR Leads in Academies will oversee and monitor the process of carrying out DPIAs.

8.3. 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.

8.4. In assessing levels of risk, the likelihood and severity of any impact on individuals must always be considered.

8.5. If and when a high risk is identified that cannot be mitigated, the DPO will consult with the Information Commissioner's Office (ICO) prior to the commencement of processing of the biometric data.

8.6. The ICO will provide the Trust and/or an Academy with a written response (within eight weeks or 14 weeks in complex cases) advising whether the risks are acceptable, or whether there is further action required. In some cases, the ICO may advise not carry out the processing.

8.7. The Trust will adhere to any advice received from the ICO.

9. Providing Consent for use of Biometric Information

9.1. 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 GDPR but is required by provisions in Section 26 of the Protection of Freedoms Act 2012.

9.2. In order to use staff and pupil biometric data as part of an automated biometric recognition system, the Trust must comply with the provisions set out in the Protection of Freedoms Act 2012.

9.3. The Academy must obtain written consent from at least one parent of the pupil before the Academy collects or uses any pupil biometric data. In Appendix 3 there are examples of the type of letter and consent form that Academies may use in obtaining consent.

9.4. The name and contact details of the pupil's parent/s will be taken from the Academy's Pupil Admissions Register.

9.5. Where the name of only one parent is included on the Admissions Register, the Headteacher/Head of School will consider whether any reasonable steps can or should be taken to ascertain the details of the other parent.

9.6. The Trust does not need to notify a particular parent or seek their consent if it is satisfied that:

- The parent cannot be found, e.g., their whereabouts or identity is not known.
- The parent lacks the mental capacity to object or consent.
- The welfare of the pupil requires that a particular parent is not contacted, e.g.. where a pupil has been separated from an abusive parent who must not be informed of the pupil's whereabouts.
- It is otherwise not reasonably practicable for a particular parent to be notified or for their consent to be obtained.

9.7. Where neither parent of a pupil can be notified for any of the reasons set out above, consent will be sought from the following individuals or agencies as appropriate:

- If a pupil is being 'looked after' by the 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 and written consent will be obtained from at least one carer before the pupil's biometric data can be processed.

9.8. Notification sent to parents and other appropriate individuals or agencies will include information regarding the following:

- The exact 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 Trust's duty to provide reasonable alternative arrangements for those pupils whose information cannot be processed.

9.9. The Trust 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

9.10. Parents and pupils can object to participation in a biometric system(s) or withdraw their consent at any time. Where consent is withdrawn any biometric data relating to the pupil that has already been captured will be deleted. A record of the erasure of the data will be date and time stamped.

9.11. If a pupil objects or refuses to participate, or to continue to participate, in activities that involve the processing of their biometric data, the Trust will ensure

that 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(s).

10. Reasonable alternatives to the use of biometric data.

10.1. The use of biometric data in Academies must always be with explicit consent and meet requirements laid out in this policy. There must also be available an alternative, which is a genuine and non-prejudicial alternative.

10.2. The Trust must ensure that parents, pupils, staff members and other relevant adults have the right to not take part in the Trust/Academy's biometric system(s) by having access to an alternative.

10.3. For example, a cashless catering system for pupils can give pupils a PIN code to use instead of requiring use biometric data for scanning when purchasing refreshments from the canteen.

10.4. An alternative system used should not place the pupil or staff member at any disadvantage in accessing the relevant service.

11. Responsibilities

11.1. All staff of the Saint Ralph Sherwin Catholic Multi Academy Trust have a responsibility to uphold this policy and take time to read and understand this policy.

11.2. Headteachers and GDPR leads in Academies must ensure that requirements set out in this policy are implemented consistently and with rigor across the Academy.

11.3. The Trust Data Protection Officer (DPO) is responsible for:

- Monitoring the Trust 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 Trust/Academy's biometric system(s)
- Being the first point of contact for the ICO and for individuals whose data is processed by the Trust/Academy and connected third parties.

11.4. The Head of Governance, Estates and Facilities Manager and CEO are responsible for supporting Headtaechers and senior leaders with the implementation of this policy.

12. Monitoring, Compliance and Review

12.1. The Finance and Estates Committee has overall responsibility for monitoring and reviewing the impact of this policy and making recommendations for updates and

revisions as needed, or when there are changes in regulations and legislation that the Trust must respond to.

12.2. The Finance and Estates Committee will review and sign off this policy annually. If during the year legislation or requirements change, then the Trust will update this policy before the next annual review.

12.3. This policy will be published on the Trust website.

12.4. Each Academy will publish the policy and their respective Academy website in their policy section.

Appendix 1: Further Information and Guidance

Further information and guidance about data protection and the protection of biometric information of pupils in schools can be found using the following links below:

Department for Education (DfE, 2018) - Protection of Biometric Information of Children in Schools – Advice for proprietors, governing bodies, head teachers, principals and school staff: https://www.gov.uk/government/publications/protection-of-biometric-information-ofchildren-in-schools

Information Commissioners Office (ICO) - Guidance on data protection for education establishments: https://ico.org.uk/for-organisations/in-your-sector/education/

Appendix 2: Biometrics Frequently Asked Questions

What is "biometrics"?
Biometrics is a method of recognizing an individual based on measurable biological characteristics such as the fingerprint. Fingerprints remain constant over a person's lifespan. Surface wear, minimal temporary or permanent scarring and aging may affect but does not alter beyond recognition, the original fingerprint pattern.

How is a biometric collected?
Sensors are used to scan the finger and convert the information to a secure digital format to which it is later compared. Technically, biometric capture devices (such as the device we will be using called an M2-Hamster Plus) create electronic digital "pictures" that are encrypted and stored and then compared to "live" pictures in order to confirm the identity of a person.

Is biometric technology safe to use?
Any health concerns are actually similar to those encountered in everyday life (touching a fingerprint sensor is equivalent to touching a doorknob). Biometric systems use ordinary computing and video technology that a person typically encounters in their day-to-day activities. Biometrics requires only the placement of a finger.

If I provide my biometric (fingerprint), who has access to it and the information associated with it?
The fingerprint scan is stored in a database on one computer at the school in a proprietary format (an actual copy of the fingerprint image itself is NOT stored). Only the fingerprint reader can recognize this format. Fingerprints are not transferred to any other systems.

Can my biometric image be used anywhere other than the Academy?
No. A fingerprint registered on one system will not be valid for another unique system. Only information stored on the database linked to the biometric scanner used is available when a fingerprint is scanned.

What if the biometric scanner is stolen?
Data is not stored on the scanner itself. The scanner is a vehicle used to confirm the authenticity of the fingerprint.

Can someone steal my biometric (fingerprint)?
A fingerprint is unique. No two people have identical fingerprints. It would be next to impossible for someone to steal someone else's biometric (fingerprint).

Appendix 3: An example letter that can be used to obtain consent with a consent form.

EXAMPLE ONLY

Dear Parents/Guardian

Why are you planning to use biometrics?
The biometric identification systems operated at XXX Academy will use the finger and its image to uniquely identify each student and member of staff. The system measures many aspects of the finger to do this. Each student has their fingerprint registered, which will then be translated to a unique identification code which is entered into the system. ***The system does not create or store an image of the fingerprint.***

When a student uses the biometric identification systems, they are identified by their identification code. This form of identification is called Biometrics, which translated means measurements of human characteristics. ***This is not fingerprinting.*** *The image of the fingerprint itself is not recorded or stored and cannot be regenerated from the digital data which cannot, therefore, be compared to existing records of fingerprint images.*

Parental consent is required to take and process biometric data from your child's finger and use this information for the purpose of providing your child with certain services, such as the cashless system used in the canteen. We will not use the biometric information for any purpose other than the in the cafeteria and in the library. XXX School will store the biometric information collected securely in compliance with the Data Protection Act 2018. We will only share this information with the suppliers of our biometric identification systems and will not unlawfully disclose it to any other person.

In order to be able to use your child's biometric information in this way, ***parental consent is required****. Attached to this letter is a consent form which requires signing and returning to your child's tutor to enable your child to continue to use the library and canteen biometric systems. You can withdraw your consent at any time by writing to us. In addition, your child may at any time object or refuse to allow their biometric information to be used even if you have given your consent. We would appreciate it if could you explain this to your child.*

If you do not wish your child's biometric information to be processed by the Academy, or your child objects to such processing, we will provide, where possible, reasonable alternative arrangements that allow them to access the relevant services.

Should you agree to the processing of your child's biometric information, please note that when he/she leaves the Academy, or if for some other reason he/she ceases to use the biometric system, his/her biometric data will be deleted.

Attached to this letter is a frequently asked questions guide for parents/guardians however, if you require further information then please feel free to contact XXXX.
Yours faithfully

EXAMPLE ONLY

BIOMETRIC IDENTIFCATION CONSENT FORM

I am aware that XXX Academy is using **biometric finger scan technology** in the cafeteria and in the library**.**

I /We give our consent for my/our child to participate in the scheme. ☐

I / We do not want my/our child to participate in the scheme. ☐

Print name of student: …… **Tutor Group**……

Print name of parent/guardian: ……

Date: ……

Signature of Parent/Guardian: ……