DIOCESE OF SOUTHWELL AND NOTTINGHAM MULTI ACADEMY TRUST

BIOMETRIC DATA PROTECTION POLICY

Approved by the Board of Directors February 2026

Policy:	Biometric Data Protection Policy
Approved by:	SNMAT Board of Directors
Date:	February 2026
Review cycle:	Annual

VERSION CONTROL			
VERSION	**DATE**	**AUTHOR**	**CHANGES**
2026	January 2026	SKP/MH	New policy

1. Introduction

The Diocese of Southwell and Nottingham Multi-Academy Trust (the Trust) is committed to protecting the privacy and rights of pupils, staff, parents, and visitors. Biometric data is recognised as special category personal data under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This policy sets out the Trust's approach to the collection, use, storage, and deletion of biometric data, ensuring compliance with legal requirements and best practice guidance from the Information Commissioner's Office (ICO).

2. Definition of Biometric Data

Biometric data includes any personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of an individual, which allows or confirms their unique identification. This may include facial recognition data, fingerprints, iris scans, voice recognition, or behavioural patterns.

3. Principles for the Use of Biometric Data

The Trust will only consider the use of biometric systems where there is a clear, proportionate, and evidenced justification; where less intrusive alternatives cannot reasonably achieve the same purpose; and where the rights and freedoms of individuals are fully protected. The Trust acknowledges the ICO's concerns regarding the use of facial recognition technology in schools and will apply these considerations to any proposed biometric processing.

4. Legal Basis for Processing

Biometric data is special category personal data and requires both a lawful basis under Article 6 UK GDPR and a special category condition under Article 9 UK GDPR. For pupils under the age of 13, explicit written consent must be obtained from parents/carers before any biometric data is collected or processed. In most cases, the Trust will seek consent from both parents unless only one parent has parental responsibility or obtaining both consents is not reasonably practicable. Pupils aged 13 and over may provide their own consent if they have sufficient understanding of the processing and their rights. Consent must be freely given, informed, specific, and capable of being withdrawn at any time. A genuine, non-biometric alternative must always be offered without detriment.

5. Prohibition on Automated Decision-Making

Biometric data will not be used for automated decision-making or profiling. It will only be used for the specific purpose for which consent was obtained.

6. Data Protection Impact Assessment (DPIA)

Before any biometric system is introduced, the Trust will complete a full DPIA assessing necessity, proportionality, risks, alternatives, and consultation with affected individuals. No biometric system may be deployed without written approval from the Trust's Data Protection Officer (DPO).

7. Consent Requirements

For pupils under 13, written consent will normally need to be obtained from both parents before any biometric data is collected or processed. Where only one parent has parental responsibility, or where obtaining consent from both parents is not reasonably practicable, the Trust will document the reasons and ensure the decision is lawful and appropriate. Pupils aged 13 and over may give their own consent if they have sufficient maturity and understanding. Any pupil may object at any time, and their objection overrides parental consent. No pupil will be disadvantaged if they do not consent. Where biometric data is collected or processed for adults, clear information will be presented on why data is being processed, and they may refuse or withdraw consent at any time.

8. Alternatives to Biometric Systems

The Trust will always provide a non-biometric alternative that is genuine, practical, and free from disadvantage or stigma. Biometric systems will never be the sole method of access or identification.

9. Data Security and Storage

Where we store the data, biometric information will be secured with industry standard strong encryption, accessible only to authorised personnel, and processed solely for the purpose for which consent was given. Any servers that store biometric data will have up-to-date anti-virus/anti-ransomware software, be in a physically secure location and have access permissions restricted to authorised users. Raw biometric images will not be stored unless strictly necessary. Unless to provide key services to pupils, staff, parents, and visitors or where legally required, data will not be shared with third parties.

10. Retention and Deletion

Biometric data will be retained only for as long as necessary. It will be deleted when consent is withdrawn, when the individual leaves the Trust, or when the system is no longer required. Deletion must be secure and irreversible.

11. Data Breaches

Any suspected or actual breach involving biometric data must be reported immediately to the Academy Data Protection Co-ordinator, logged onto the Trust IT Helpdesk, escalated to the Trust IT Manager and DPO, and investigated promptly. Biometric data breaches are considered high-risk.

12. Roles and Responsibilities

Academy Data Protection Co-ordinator: Local oversight and reporting. Headteacher: Ensures academy-level implementation. Academy IT Manager/Network Manager/Senior IT Engineer: Ensures academy-level implementation and security. Trust IT Manager: Provides technical assistant to DPIAs, implementations and integrations and overseas technical security. Data Protection Officer: Provides advice, approves DPIAs, and oversees compliance.

13. Monitoring and Review

This policy will be reviewed annually or sooner if legislation changes, ICO guidance is updated, new technologies are proposed, or incidents indicate a need for revision.

Appendix A

Catering System – Biometric Data Data Protection Impact Assessment

DIOCESE OF SOUTHWELL & NOTTINGHAM
MULTI ACADEMY TRUST

Approved by the Board of Directors February 2026

Versions:			
VERSION	**DATE**	**AUTHOR**	**CHANGES**
2026	JAN 2026	MJH – Trust IT Manager	Example based upon the ICO DPIA template 2018.

Submitting controller details

Name of controller	Diocese of Southwell & Nottingham Multi-Academy Trust
Subject/title of DPO	Microsoft Copilot Chat for Education
Name of controller contact /DPO (delete as appropriate)	Sarah Perry

Step 1: Identify the need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
The academy proposes to introduce a biometric identification system to support cashless catering. The system will allow staff and pupils to authenticate their identity using biometric data (e.g., fingerprint or facial recognition) to purchase meals quickly and securely. The purpose is to improve efficiency, reduce queue times, minimise the handling of cash, and ensure accurate allocation of meals, including free school meal entitlement. A DPIA is required because special category information is processed on a large scale, and data subjects must be fully aware of how their data is used.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?
Nature of Processing: Collection of biometric data, storage of encrypted templates, use for identity verification, secure deletion. **Categories of Data Subjects:** Pupils and staff (if included). **Categories of Personal Data:** Biometric data, name, unique pupil number, meal entitlement status. **Special Category or High Risk Data:** Yes – biometric data.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?
Biometric data is considered special category information, and collection would be limited to face or fingerprint for identification. Data will be retained for the period of employment or enrolment within the school and removed on close of that employment or enrolment. All individuals within the school community who wish to use the catering provided would be affected.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?
Individuals are members of the school community (including children) who wish to use the provided catering functions. They have full control over their consent to using biometric systems and may withdraw it at any time without penalty. Use of biometrics is a modern, secure and streamlined way to speed monetary transactions, especially for young people to avoid the need of other mechanisms such as cash or cards. Technology is mature and robust, as long as data security is paramount and processing is legally justified.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?
Purpose: To enable efficient, secure, and accurate catering transactions.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?
Consultation should take place with the Data Protection Officer, CEO and Trust IT Manager and Academy Headteachers. Consent Requirements: For pupils under 13, written consent must be obtained from parents/carers, normally both. Pupils aged 13+ may consent if competent. Consent must be freely given and withdrawable. Alternatives must be offered. Consideration of alternatives, proportionality, ICO concerns, data minimisation, and transparency.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?
Lawful Basis (Article 6): Consent. **Special Category Condition (Article 9):** Explicit consent.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Misuse Of Biometric Data	Medium	High	High
Data Breach	Medium	High	High
Consent Not Given	Medium	High	High
Technical Failure	Medium	Low	Low
Data Retained			

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
Misuse Of Biometric Data	Data is fully encrypted, with access only granted for lawful processing. No raw images are stored with clear staff training and guidance.	Reduced	Low	
Data Breach	Data is stored on encrypted servers, up-to-date with security and anti-ransomware tools, with access limited to specific admin accounts.	Reduced	Medium	
Consent Not Given	Clear consent information provided, with an alternative non-biometric option offered where available.	Reduced	Low	

Step 7: Sign off and record outcomes

Item	**Name/position/date**	**Notes**
Measures approved by:	Sarah Perry	
Residual risks approved by:	Sarah Perry	
DPO advice provided:		
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons

Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA

Appendix B

DIOCESE OF SOUTHWELL & NOTTINGHAM MULTI ACADEMY TRUST

CONFIDENTIAL PARENTAL CONSENT FORM

Use of Biometric Systems Permission Form

*If the academy uses biometric systems (e.g. fingerprint / palm recognition technologies) to identify children for access, attendance recording, charging, library lending etc. it must (under the GDPR legislation) seek permission from **both** parents or carers.*

The academy uses biometric systems for the recognition of individual children/students in the following ways (the school should describe here how it uses the biometric system).

Biometric technologies have certain advantages over other automatic identification systems as pupils do not need to remember to bring anything with them (to the canteen or school library) so nothing can be lost, such as a swipe card.

The academy has carried out a privacy impact assessment and is confident that the use of such technologies is effective and justified in an academy context.

No complete images of fingerprints/palms are stored and the original image cannot be reconstructed from the data. That is, it is not possible for example, to recreate a pupil's fingerprint or even the image of a fingerprint from what is in effect a string of numbers.

Parents / carers are asked for permission for these biometric technologies to be used by their child:

Parent / Carers Name: .....

Student / Pupil Name: .....

As the parent / carer of the above student / pupil, I agree to the school using biometric recognition systems, as described above. I understand that the images cannot be used to create a whole fingerprint / palm print of my child and that these images will not be shared with anyone outside the school.	Yes / No

Signed: .....

Date: .....

Please note that this consent will remain in force until your child has left the school unless you rescind it. You have the right to withdraw your consent at any time by contacting the academy either by e-mail to …… or telephone …… or by contacting the Data Protection Officer at data.protection@snmat.org.uk

Approved by the Board of Directors February 2026