



Holy Family of Nazareth Catholic Academy Trust

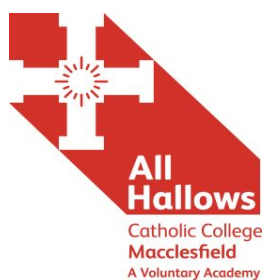
Provision of Biometric Information of Children in Schools Policy

Date of policy: October 2020

Date last review adopted by HFNCAT Board: March 2021

Frequency of review: Annually

Date of next review: October 2021



Statement of Intent

The Holy Family of Nazareth Catholic Academy Trust is committed to protecting the personal data of all its learners and staff, this includes any biometric data we collect and process.

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

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, e.g. their fingerprint.

The information will be used as part of an automated biometric recognition system. This system will take measurements of the biometric information specified above and convert these measurements into a template to be stored on the system. An image of a student's biometric information is not stored. The template (i.e. the biometric measurements taken from a child) will be used to permit students to use appropriate biometric systems within the school sites (e.g. cashless catering systems).

Providing consent/objecting to the use of biometric data

Under the Protection of Freedoms Act 2012, the Trust is required to notify each parent/guardian of a child and obtain the written consent of at least one parent/guardian before being able to use any learner's biometric information for an automated system. This is usually done when the child starts at the school. Students who are over the age of sixteen can provide their own consent. Data protection laws state a young person can consent to the processing of their personal data from when they are able to understand why it is being used.

If a young person objects the school should not process or continue to process their biometric data, irrespective of whether consent has been provided by the parent. A pupil's objection or refusal overrides any parental consent to the processing.

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
 - General Data Protection Regulation (GDPR)
 - DfE (2018) 'Protection of biometric information of children in schools and colleges'
- This policy operates in conjunction with the following policy:
 - Data Protection Policy.

Definitions

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.

Automated biometric recognition system: A system 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.

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 students' biometric data, e.g. taking measurements from a fingerprint via a fingerprint scanner
- Storing students' biometric information on a database
- Using students' biometric data as part of an electronic process, e.g. by comparing it with biometric information stored on a database to identify or recognise learners.

Special category data: 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.

Roles and Responsibilities

- The Holy Family of Nazareth Catholic Academy Trust Board is responsible for reviewing this policy on an annual basis.
- The Principal / Headteachers, in conjunction with the school GDPR Lead person, are responsible for ensuring the provisions in this policy are implemented consistently.
- The Data Protection Officer (DPO) is responsible for:
 - Monitoring the Trust's 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's biometric systems.
 - Being the first point of contact for the ICO and for individuals whose data is processed by the Trust and connected third parties.

Data Protection Principles

The HFNCAT processes all personal data, including biometric data, in accordance with the key principles set out in the GDPR. The Trust ensures biometric data is:

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

The Trust is responsible for being able to demonstrate its compliance with the provisions outlined above.

Data Protection Impact Assessments (DPIAs)

- Prior to processing biometric data or implementing a system that involves processing biometric data, a DPIA will be carried out
- The GDPR Lead in each school in conjunction with the DPO will oversee and monitor the process of carrying out the DPIA
- 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
- When assessing levels of risk, the likelihood and the severity of any impact on individuals will be considered
- 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 in complex cases) advising whether the risks are acceptable, or whether the academy needs to take further action. In some cases, the ICO may advise the academy to not carry out the processing

- The Holy Family of Nazareth Catholic Academy Trust will adhere to any advice received from the ICO

Notification and Consent

Please note that the obligation to obtain consent for the processing of biometric information of young people under the age of 18 is not imposed by the Data Protection Act 2018 or the GDPR. Instead, the consent requirements for biometric information is imposed by section 26 of the Protection of Freedoms Act 2012.

- Where The Holy Family of Nazareth Catholic Academy Trust use learners' biometric data as part of an automated biometric recognition system (e.g. using students' fingerprints to receive school dinners instead of paying with cash or a PIN), The Holy Family of Nazareth Catholic Academy Trust will comply with the requirements of the Protection of Freedoms Act 2012.
- Prior to processing a student's biometric data, the school will send the parents/guardian a Student Consent Form.
- Written consent will be sought from at least one parent/guardian of the student before the school collects or uses their biometric data.
- Notification sent to parents/guardians will include information regarding the following:
 - How the data will be used
 - The parent's/guardian's and the student's right to refuse or withdraw their consent
 - The school's duty to provide reasonable alternative arrangements for those students whose information cannot be processed
- The academy will not process the biometric data of a student under the age of 18 in the following circumstances:
 - The student (verbally or non-verbally) objects or refuses to participate in the processing of their biometric data
 - No parent/guardian has consented in writing to the processing
 - A parent/guardian has objected in writing to such processing, even if another parent has given written consent
- Parents/guardians and students can object to participation in the academy's biometric system(s) or withdraw their consent at any time. Where this happens, any biometric data relating to the learner that has already been captured will be deleted.
- If a student objects or refuses to participate, or to continue to participate, in activities that involve the processing of their biometric data, their home school will ensure that their biometric data is not taken or used as part of a biometric recognition system, irrespective of any consent given by the parent/guardian(s).

- Students will be informed that they can object or refuse to allow their biometric data to be collected and used via the Consent Form.
- Where staff members or other adults use the biometric system(s), consent will be obtained from them before they use the system.
- Staff and other adults can object to taking part in the 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.
- Alternative arrangements will be provided to any individual that does not consent to take part in the Holy Family of Nazareth Catholic Academy Trust biometric system(s), in line with the next section of this policy.

Alternative Arrangements

Students and staff have the right to not take part in the Holy Family of Nazareth Catholic Academy Trust biometric system.

Where an individual person objects to taking part in the biometric system(s), reasonable alternative arrangements will be provided that allow the individual to access the relevant service.

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 student's parents, where relevant).

Data Retention

If an individual (or a student's parent, where relevant) withdraws their consent for their/their child's biometric data to be processed, it will be erased from the academy's system.

Breaches

There are appropriate and robust security measures in place to protect the biometric data held by the academy as part of the GDPR processes in place. In the unlikely event of a breach to the biometric system(s), it will be dealt with by the Holy Family of Nazareth Catholic Academy Trust DPO.

Signed

Chair of Holy Family of Nazareth Catholic Academy Trust Board

Date