Our mission - 'To create and sustain an inclusive and outstanding learning community for all, rooted in the teachings of Jesus Christ, in which all will aspire to excellence in learning, teaching and care for one another, so all will achieve and grow as unique individuals madein the image of God'.

Our Core Values;

Faith, Aspiration & Unity

We are committed to providing a positive working environment which is free from prejudice and unlawful discrimination and any form of harassment, bullying or victimisation. We have developed a number of key policies to ensure that the principlesof Catholic and Church of England Social Teaching in relation to human dignity and dignity in work become embedded into every aspect of school life and these policies arereviewed regularly in this regard.

PROTECTION OF BIOMETRIC INFORMATION POLICY

Protection of Biometric Information Policy - Document Status			
Date of review completion	May 2025	**Named Responsibility**	Buildings, Health & Safety and SafeguardingCommittee (JH)
Date of Policy Adoption by Governing Body	May 2025	**Next Review Date**	May 2026
Policy Basis	From School bus Website - Adapted for HTA		

Contents:

Statement of intent

1. Legal framework
2. Definitions
3. Roles and responsibilities
4. Data protection principles
5. Data protection impact assessments (DPIAs)
6. Notification and consent
7. Alternative arrangements
8. Data retention
9. Breaches
10. Monitoring and review

Statement of intent

Holy Trinity Academy 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 relevant legislation and guidance to ensure the data and the rights of individuals are protected. This policy outlines the procedure the school follows when collecting and processing biometric data.

1. Legal framework

1.1. 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 (2022) 'Protection of biometric information of children inschools and colleges'

1.2. This policy operates in conjunction with the following school policies:

- Data Protection Policy
- Records Management Policy

2. Definitions

2.1. **Biometric data:** Personal information about an individual's physical or behavioral characteristics that can be used to identify that person, including their fingerprints, facial shape, retina and iris patterns, and hand measurements.

2.2. **Automated biometric recognition system:** A system which measures an individual's physical or behavioral characteristics by using equipment that operates 'automatically' (i.e. electronically). Information from the individual is automatically compared with biometric informationstored in the system to see if there is a match in order to recognise or identify the individual.

2.3. **Processing biometric data:** Processing biometric data includes obtaining, recording or holding the data or carrying out any operation onthe data including disclosing it, deleting it, organising it or altering it. An automated biometric recognition system processes data when:

- Recording pupils' biometric data, e.g. 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, e.g. by

comparing it with biometric information stored on a database to identify or recognise pupils.

2.4. **Special category data:** Personal data which the GDPR says is more sensitive, and so needs more protection – where biometric data is usedfor identification purposes, it is considered special category data.

3. Roles and responsibilities

The governing board is responsible for reviewing this policy on an **annual** basis.

The Headteacher is responsible for ensuring the provisions in this policy are implemented consistently.

The DPO is responsible for:

- Monitoring the school's compliance with data protection legislation in relation to the use of biometric data.
- Identifying the additional risks associated with using automated biometric technology by conducting a data protection impact assessment (DPIA).
- Being the first point of contact for the ICO and for individuals whose data is processed by the school and connected third parties.

4. Data protection principles

4.1. The school processes all personal data, including biometric data, in accordance with the key principles set out in the GDPR.

4.2. The school ensures biometric data is:

- Processed lawfully, fairly and in a transparent manner.
- Only collected for specified, explicit and legitimate purposes, andnot further processed in a manner that is incompatible with thosepurposes.
- Adequate, relevant and limited to what is necessary in relation tothe 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 nolonger 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.

4.3. As the data controller, the school is responsible for being able to demonstrate its compliance with the provisions outlined in 4.2.

5. Data protection impact assessments (DPIAs)

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

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

5.3. 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.

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

5.5. If a high risk is identified that cannot be mitigated, the DPO will consult the ICO before the processing of the biometric data begins.

5.6. The ICO will provide the school with a written response (within eight weeks or 14 weeks in complex cases) advising whether the risks are acceptable, or whether the school needs to take further action. In somecases, the ICO may advise the school to not carry out the processing.

5.7. The school will adhere to any advice from the ICO.

6. Notification and consent

Please note that 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 Act2018 or the GDPR. Instead, the consent requirements for biometric information is imposed by section 26 of the Protection of Freedoms Act 2012.

6.1. Where the school uses pupils' biometric data as part of an automated biometric recognition system (e.g. using pupils' fingerprints to receive school dinners instead of paying with cash), the school will comply withthe requirements of the Protection of Freedoms Act 2012.

6.2. Prior to any biometric recognition system being put in place or processing a pupil's biometric data, the school will send the pupil's parents a Parental Notification and Consent Form for the use of Biometric Data.

6.3. Written consent will be sought from at least one parent of the pupil before the school collects or uses a pupil's biometric data.

6.4. The name and contact details of the pupil's parents will be taken from the school's admission register.

6.5. Where the name of only one parent is included on the admissions register, the Headteacher will consider whether any reasonable steps can or should be taken to ascertain the details of the other parent.

6.6. The school 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 abusiveparent who must not be informed of the pupil's whereabouts.
- It is otherwise not reasonably practicable for a particular parent tobe notified or for their consent to be obtained.

6.7. Where neither parent of a pupil can be notified for any of the reasons set out in 6.6, 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 fromat least one carer before the pupil's biometric data can be processed.

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

- 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 theirconsent
- The school's duty to provide reasonable alternative arrangementsfor those pupils whose information cannot be processed

6.9. 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 toparticipate 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 ifanother parent has given written consent

6.10. Parents 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.

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

6.12. Pupils will be informed that they can object or refuse to allow their biometric data to be collected and used via a letter.

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

6.14. Staff and other adults can object to taking part in the school's biometricsystem(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.

6.15. Alternative arrangements will be provided to any individual that does notconsent to take part in the school's biometric system(s), in line with section 7 of this policy.

7. Alternative arrangements

7.1. Parents, pupils, staff members and other relevant adults have the right to not take part in the school's biometric system(s).

7.2. 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, e.g. where a biometric system uses pupil's fingerprints to pay for school meals, the pupil will be able to use cash for the transaction instead.

7.3. Alternative arrangements will not put the individual at any disadvantageor create difficulty in accessing the relevant service, or result in any additional burden being placed on the individual (and the pupil's parents,where relevant).

8. Data retention

8.1. Biometric data will be managed and retained in line with the school's Records Management Policy.

8.2. The school will only store and process biometric information for the purpose for which it was originally obtained and consent provides.

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

9. Breaches

9.1. There are appropriate and robust security measures in place to protectthe biometric data held by the school. These measures are detailed in the school's Data Protection Policy.

9.2. Any breach to the school's biometric system(s) will be dealt with inaccordance with the Data Protection Policy.

10. Monitoring and review

10.1. The governing board will review this policy on an annual basis.

10.2. The next scheduled review date for this policy is May 2026.

10.3. Any changes made to this policy will be communicated to all staff,parents and pupil