HEARTWOOD
LEARNING TRUST

PROTECTION OF BIOMETRIC INFORMATION POLICY

THIS POLICY APPLIES TO ALL SCHOOLS/ACADEMIES WITHIN HEARTWOOD LEARNING TRUST WHO PROCESS BIOMETRIC DATA

THIS POLICY SHOULD BE USED IN CONJUNCTION WITH THE DATA PROTECTION (UK GDPR) POLICY AND IS SUPPORTED BY APPROPRIATE DATA PROTECTION IMPACT ASSESSMENTS

Document Management	
Updated Policy Approved	June 2025
Next Review Date	June 2027
Version	1.6
Approved By	Chief Operating Officer

Contents

Policy Updates

Date	Page	Policy Updates
April 2023	5	1.1 - Legal framework updated to reflect current legislation and guidance
April 2023	5	2.1 - Point reworded under 'definitions'
April 2023	6	3.3 - Bullet point added re: DPO responsibilities
April 2023	9	8.2 - Point added re: data retention
April 2023	13	Consent Form for the Use of Biometric Information re-formatted in line with other Trust localised appendices
November 2023	Whole policy	Updated inline with the new Scheme of Delegation
March 2024	4	Statement of intent wording updated
June 2025	4	Introduction added in line with other Trust policies
June 2025	4	Statement of Intent - Minor wording amendments
June 2025	5	1.2 - Legal Framework updated to reflect applicable Trust policies
June 2025	7	4.3 - Point updated to refer to other Trust policy
June 2025	7	5.7 - Point added regarding DPIAs being reviewed regularly
June 2025	8	6.8 - Reference to LAC changed to CIC to reflect current policy

Introduction

Heartwood Learning Trust is an inclusive and collaborative Church of England multi-academy trust serving church, community and alternative provision schools. This policy is guided by our Christian ethos and the visions of our Trust and its schools/academies. We share a clear vision – to create schools where children and young people thrive, as we help them prepare to live life in all its fullness (John 10:10).

For us, a place to thrive means much more than a place simply to be comfortable. Instead, our aim is to develop schools and an educational offer which enable each pupil to flourish academically, practically, emotionally, socially and spiritually.

Statement of Intent

Heartwood Learning Trust is committed to protecting the personal data of all its pupils, parents/carers, employees and volunteers, including any biometric data processed by the Trust or its schools/academies.

The Trust and its schools/academies collect and process biometric data in accordance with relevant legislation and guidance to ensure the data and the rights and freedoms of all Data Subjects are protected. We will treat the personal data collected with appropriate care and ensure that security measures are in place to limit access to biometric data processed by the Trust/school/academy. This policy outlines the procedure the Trust/school/academy follows when collecting and processing biometric data.

1. Legal Framework

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

- Protection of Freedoms Act 2012
- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR)
- DfE (2022) 'Protection of biometric information of children in schools and colleges'
- DfE (2023) 'Data Protection in Schools'

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

- Data Protection (UK GDPR) Policy (including the Data Retention Schedule)
- Data Breach Policy and Procedures
- E-Safety and Acceptable Use Policies
- UK GDPR Privacy Notices

2. Definitions

2.1. **Biometric data** is considered special category data and refers to personal information, resulting from specific technical processing, about an individual's physical or behavioural characteristics that can be used to identify that person via a digital reading (**not** image), including (but not limited to) their fingerprint, facial shape, retina and iris patterns, and hand measurements. All biometric data is personal data.

2.2. An **'automated biometric recognition system'** is 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. Biometric recognition systems can use many kinds of physical or behavioural characteristics, such as those listed above.

2.3. **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, e.g. taking a digital reading from a fingerprint via a 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:** This is sensitive personal data which, according to the UK GDPR requires more protection - where biometric data is used for identification purposes, e.g. through keystroke analysis, it is considered special category data.

3. Roles and Responsibilities

3.1. The **Compliance Officer** is responsible for:

- Reviewing this policy on an annual basis prior to approval from the **Chief Operating Officer**
- Reviewing any data protection impact assessments (DPIAs) provided by the school/academy in relation to their use of biometric data systems, e.g. cashless catering prior to final approval by the **Data Protection Officer (DPO)**
- Providing support to the **DPO**, as necessary in the monitoring of data protection performance
- Ensuring that nominated **GDPR Representatives** in schools/academies receive appropriate training on data protection on a regular basis

3.2. The **Principal** is responsible for:

- Ensuring the provisions in this policy are implemented consistently
- Obtaining approval from the **Data Protection Officer (DPO)** prior to any systems being sourced or investigated
- Ensuring that a data protection impact assessment (DPIA) in relation to the school/academy's biometric system(s) is undertaken prior to implementation and reviewed periodically

3.3. The **Data Protection Officer (DPO)** is responsible for:

- Monitoring the school/academy'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)
- Approval, in advance, of any proposed new software
- Review and approval of Data Protection Impact Assessments (DPIAs) in relation to the school/academy's biometric system(s)
- Being the first point of contact for the **Information Commissioner's Office (ICO)** and for individuals whose data is processed by the school/academy and connected third parties

4. Data Protection Principles

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

4.2. The school/academy 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

4.3. As the data controller, the school/academy is responsible for being able to demonstrate its compliance with the provisions outlined above. Further information on how the Trust processes personal data in line with data protection principles can be found within our **Privacy Notices**.

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 **Principal** will oversee and monitor the process of carrying out the DPIA, in correspondence with the **Data Protection Officer (DPO)** and **Compliance Officer**, and submit for review prior to use or in the event of amendments.

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
- Be reviewed frequently and kept updated

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/academy with a written response (within eight weeks or 14 weeks in complex cases) advising whether the risks are acceptable, or whether the school/academy needs to take further action. In some cases, the **ICO** may advise the school/academy to not carry out the processing. The school/academy will adhere to any advice provided from the **ICO**.

5.7. The Trust will treat each DPIA as a 'live' document to ensure the risks of processing personal data, including biometric data, are reviewed and managed effectively. DPIAs will be reviewed every two years or in response to any changes.

6. Notification and Consent

6.1. **Please note:** the obligation to obtain consent for the processing of biometric data 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 are imposed by section 26 of the Protection of Freedoms Act 2012.

6.2. Where the school/academy uses biometric data as part of an automated biometric recognition system (e.g. using pupils' and employees' biometric fingerprint recognition for the purposes of cashless catering), the school/academy will comply with the requirements of the Protection of Freedoms Act 2012.

6.3. Prior to any biometric recognition system being put in place or processing a pupil's biometric data, the school/academy will send the pupil's parents/carers a **Parental Notification and Consent Form for the use of Biometric Data** (Appendix A).

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

6.5. The name and contact details of the pupil's parents/carers will be taken from the school/academy's admission register.

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

6.7. The school/academy does not need to notify a particular parent/carer or seek their consent if it is satisfied that:

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

6.8. Where no parent/carer of a pupil can be notified for any of the reasons set out in 6.7, consent will be sought from the following individuals or agencies as appropriate:

- If a pupil is classed as a Child in Care (CIC) by the Local Authority (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

6.9. Notification sent to parents/carers 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
- How the data will be stored
- The parent/carer's and the pupil's right to refuse or withdraw their consent
- The school/academy's duty to provide reasonable alternative arrangements for those pupils whose information cannot be processed

6.10. The school/academy 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/carer has objected in writing to such processing, even if another parent/carer has given written consent

6.11. Parents/carers and pupils will be made aware that they can object to participation in the school/academy's biometric system(s) or withdraw their consent at any time, and that if they do this, the school/academy will provide them with an alternative method of accessing the relevant services. The steps taken by the school/academy to inform pupils will take account of their age and level of understanding. Parents/carers will also be informed of their child's right to object and will be encouraged to discuss this with their child.

6.12. Where a pupil or their parents/carers object or withdraws their consent, any biometric data relating to the pupil that has already been captured will be deleted. 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/academy 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/carer(s).

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

6.14. Employees and other adults can object to taking part in the school/academy'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.

6.15. Alternative arrangements will be provided to any individual that does not consent to take part in the school/academy's biometric system(s), in line with section 7 of this policy.

7. Alternative Arrangements

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

7.2. Where an individual objects to taking part in the school/academy'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 fingerprint recognition to pay for school meals, the pupil will be given an alternative means to enable them to make purchases i.e. codes etc.

7.3. 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).

8. Data Retention

8.1. Biometric data will be managed and retained in line with the Trust's **Data Protection (UK GDPR) Policy** (including the **Data Retention Schedule**).

8.2. The Trust will only store and process biometric information for the purpose for which it was originally obtained and consent provided for from the parent/carer.

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

9. Breaches

9.1. There are appropriate and robust security measures in place to protect the biometric data held by the school/academy. These measures are detailed in the Trust's **Data Protection (UK GDPR) Policy** (including the **Data Retention Schedule**), the **Data Breach Policy and Procedures** and the **E-Safety and Acceptable Use Policies**.

9.2. Any breach to the school/academy's biometric system(s) will be dealt with in accordance with the Trust's **Data Protection (UK GDPR) Policy** (including the **Data Retention Schedule**), the **Data Breach Policy and Procedures** and the **E-Safety and Acceptable Use Policies**.

10. Monitoring and Review

10.1. The Trust's **Compliance Officer** will review this policy every two years, or earlier if there is a change in legislation/guidance. The **Chief Operating Officer** is responsible for authorisation of this policy.

10.2. The next scheduled review date for this policy is recorded on the cover page.

10.3. Any changes made to this policy will be communicated to all employees, parents/carers and pupils via the school/academy website.

APPENDIX A - Parental Notification of the use of Biometric Data

[The following is suggested text for a notification letter and consent form to parents/carers. You should adapt this text considering your school/academy's specific biometric system(s)]

Address line one
Address line two
Town
County
Postcode

Date

Dear **Parent/Carer**,

RE: Notification of intention to process pupils' biometric information and consent form

We are writing to notify you of the school/academy's wishes to use information about your child as part of an automated (i.e. electronically-operated) recognition system. The purpose of this system is to **[specify what the purpose of the system is, e.g. to facilitate catering transactions to be made using pupils' via fingerprint recognition instead of using cash]**.

The information from your child that we wish to use is referred to as 'biometric information'.

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. digital reading of their fingerprint. The school/academy would like to collect and use the following biometric information from your child:

- **[Specify the biometric information you want to collect and process]**

The school/academy would like to use this information for the purpose of providing your child with **[specify the purpose of using the information, e.g. so the child can pay for their school meal via fingerprint recognition]**.

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 your child's biometric information is not stored*. The template (i.e. the measurements taken from your child) will be used to permit your child to access services.

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:

- The school/academy will not use the information for any purpose other than those for which it was originally obtained and made known to the parent(s)/carers (i.e. as stated above).
- The school/academy will ensure that the information is stored securely.
- The school/academy will tell you what it intends to do with the information.
- Unless the law allows it, the school/academy will not disclose personal information to another person or body.

Please note, the school/academy has to share the information with the following bodies:

- **[Specify any third party with which the information is to be shared, e.g. the supplier of the biometric system]**

This is necessary in order to **[specify why it needs to be disclosed to the third party]**.

Providing your consent/objecting to the use of biometric data

Under the Protection of Freedoms Act 2012, UK GDPR and the Data Protection Act 2018, we are required to notify each parent/carer of a child and obtain the written consent of at least one parent/carer before being able to use a child's biometric information for an automated system.

Consent given by one parent/carer will be overridden if the other parent/carer objects in writing to the use of their child's biometric information. Similarly, if your child objects to the use of their biometric information, the school/academy cannot collect or use the information for inclusion on the automated recognition system.

You can also object to the proposed processing of your child's biometric information at any time or withdraw any consent you have previously given. Please note that you must make any consent, withdrawal of consent or objection in writing.

Even if you have given your consent, your child can object or refuse at any time to their biometric information being collected and used. We would appreciate it if you could discuss this with your child and explain to them that they can object if they want to.

The school/academy is happy to answer any questions you or your child may have – please contact **name of employee** on **contact details** with any questions.

If you do not wish for your child's biometric information to be used by the school/academy, or your child objects to such processing, the school/academy will provide reasonable alternative arrangements for pupils who are not going to use the biometric system to **[insert relevant service, e.g. pay for school meals]**.

Please note that, when your child leaves the school/academy or ceases to use the biometric system, their biometric information will be securely erased in line with the Trust's Data Protection (UK GDPR) Policy (including the Data Retention Schedule).

Please complete the form below to confirm if you do or do not consent to the collection and use of your child's biometric information and return it to the **school office** by **date**.

Kind regards,

Name

Job role

Consent Form for the Use of Biometric Information

Please complete this form to confirm whether you provide consent for the school/academy to collect and use the following biometric information relating to your child:
• **[Insert the biometric information the school intends to collect and use]**
This biometric information will be used by the school/academy for the following purpose:
• **[Specify the purpose the information will be used for, e.g. catering]**
Having read the guidance provided to me by **NAME OF SCHOOL/ACADEMY**, I (please tick your selection): ☐ **Do** consent to the processing of my child's biometric data ☐ **Do not** consent to the processing of my child's biometric data
For parents/carers that have provided consent
Please confirm that you have read and understood the following terms: • I authorise the school/academy to use my child's biometric information for the purpose specified above until either they leave the school/academy or cease to use the system. • I understand that I can withdraw my consent at any time. • I understand that, if I wish to withdraw my consent, I must do so in writing and submit this to: **INSERT SCHOOL/ACADEMY ADDRESS** or via email to: **INSERT SCHOOL/ACADEMY EMAIL ADDRESS** • I understand that once my child ceases to use the biometric system, the school/academy will securely delete my child's biometric information. ☐ I confirm that I have read and understood the terms above
For all parents/carers

Name of child:	
Name of parent/carer:	
Signature of parent/carer:	
Date:	
Please return this form to the main office by:	**DATE**