PROTECTION OF BIOMETRIC DATA POLICY

Document Management Information

Applicable to:	All staff in all Academies and Central Support Services including individuals employed by the Trust, contractors and agency staff. All Parents and Guardians
Dissemination:	The policy will be available to staff via the Trust's Policy Centre and website. The Policy is available to Parents and Guardians on our Trust website
Training:	On request
Review Frequency:	The policy will be reviewed annually. The policy will be reviewed earlier if needed in the light of new evidence, legislation and guidance
Policy Author:	Owen McColgan – Chief Executive
Executive Policy Owner:	Owen McColgan – Chief Executive
Approval by:	Level 2 – Finance, Audit and Resources Committee
Approval Date:	August 2024
Next Review Date:	September 2025

Revision History

Document Version	Description of Revision	Date Approved
V1.0	Policy Approved	September 2021
V1.1	**Minor Updates**	**November 2022**
V2	**Update**	**August 2024**

Contents

Statement of intent

The Howard Academy Trust 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 academies follow when collecting and processing biometric data.

For the purpose of this policy, 'The Howard Academy Trust' refers to 'the Trust and its academies'.

1. 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 Trust policies:
- Data Protection/GDPR Policy
- Records Management Policy
- Acceptable use of Technology Policy

2. Definitions

2.1 **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.

2.2 **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.

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 measurements from a fingerprint via a fingerprint scanner or using facial shape photography.
- 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.

2.3 **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.

3. Roles and responsibilities

3.1 The Audit, Risk Management & Policy Committee is responsible for reviewing this policy on an annual basis.

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

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

3.4 The IT Department is Responsible for implementing and maintaining technical measures to protect biometric data.

3.5 Operators are trained to understand the risks associated with use of the software and understand they are accountable. All staff using the cashless catering system are contracted staff, who the contractor is responsible for ensuring appropriate training. The Trust annually required the caterer to confirm that all staff are appropriately trained

4. Data protection principles

The academies process all personal data, including biometric data, in accordance with the key principles set out in the GDPR.

The academies ensure 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.

    - Process in a manner hat 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.
    - Data is stored on site servers. These are fully backups and antivirus in place for our servers, Servers are kept in locked areas with restricted access, access is restricted to IT Staff only.
- As the data controller, the Trust is responsible for being able to demonstrate its compliance with the provisions outlined in section 4.

5. 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 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.

Regular Review: DPIAs will be reviewed regularly and updated when necessary to reflect changes in processing activities or risks.

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 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 some cases, the ICO may advise the school to not carry out the processing.

The Trust 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 Act 2018 or the GDPR. Instead, the consent requirements for biometric information are imposed by section 26 of the Protection of Freedoms Act 2012.

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

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/carers a Parental Notification and a link for them to consent to the use of Biometric Data.

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

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

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

The academy does not need to notify a particular parent/carer 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/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 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.

6.3 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 from at least one carer before the pupil's biometric data can be processed.

6.4 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
  - The carers and the pupil's right to refuse or withdraw their consent
- The academy's duty to provide reasonable alternative arrangements for those pupils whose information cannot be processed
- 6.5 The 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 has objected in writing to such processing, even if another parent has given written consent

6.5 Parents/carers and pupils 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 pupil that has already been captured will be deleted.

6.6 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 of a biometric recognition system, irrespective of any consent given by the pupil's parent(s).

6.7 Pupils will be informed that they can object or refuse to allow their biometric data to be collected and used.

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

6.9 Staff and other adults can object to taking part in the school'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.

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

7. Alternative arrangements

7.1 Parents/carers, 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 academy's biometric system(s), reasonable alternative arrangements will be provided that allow the individual to access the relevant service. For example, where a biometric system uses pupils' fingerprints or facial shape to pay for school meals, the academy, or its third party, will provide the parent/carer with a PIN number.

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 Records Management Policy.

8.2 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 academy's system.

9. Breaches

9.1 There are appropriate and robust security measures in place to protect the biometric data held by the Trust.

9.2 Any breach to the academy's biometric system(s) will be dealt with by the academy and DPO.

9.3 Notification Timeline: The Trust will notify the ICO within 72 hours of becoming aware of a data breach involving biometric data, and affected individuals will be informed without undue delay.

10. Monitoring and review

10.1 The Protection of Biometric information Policy will be reviewed by the Finance, Audit & Resources Committee on an annual basis.

10.2 Any changes made to this policy will be communicated to all staff, parents/carers and pupils and third-party operators.