Aston Community Education Trust

ACET Protection of Biometric Data Policy

DATE: November 2024

POLICY LEAD: ACET Network Leader

AUTHOR: Matthew Sutton

APPROVED BY: Finance Risk Audit & People Committee

Excellence Equity Empowerment Esteem

DOCUMENT CONTROL		POLICY LEVEL	
APPROVED BY	FRAP COMMITTEE	APROVED DATE	18th November 2024
BUSINESS LEAD	ACET Network Leader	AUTHOR	Matthew Sutton
NEXT REVIEW DATE	November 2025	FREQUENCY	ANNUAL
VERSION NUMBER	DATE ISSUED	UPDATED INFORMATION	
V1	OCTOBER 2024	Policy has had substantial re-write and additions of supporting evidence.	

ACET Protection of Biometric Data Policy

Statement of Intent

ACET 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. We will treat the data collected with appropriate care and ensure the processing is necessary and proportionate. This policy outlines the procedure the academy follows when collecting and processing biometric data.

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
- 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'

This policy operates in conjunction with the following academy policies:

- ACET Data Protection Policy
- ACET Cyber Security, Disaster Recovery, IT Incident Management Policy
- ACET E-Safety Policy

Definitions

- **Biometric data**: Personal information resulting from specific technical processing 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, hand measurements, and voice. All biometric data is personal data.
- **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**: Includes obtaining, recording, storing, disclosing, analysing, using, deleting, organising, or modifying it.
- **Special category data**: Personal data which the UK GDPR says is more sensitive and needs more protection. Where biometric data is used for identification purposes, it is considered special category data.

Roles and Responsibilities

- **Trust Board**: Responsible for reviewing this policy annually, ensuring data protection performance is monitored regularly, and providing support to the DPO as necessary.
- **Principal**: Responsible for ensuring the provisions in this policy are implemented consistently, ensuring staff receive appropriate training on data protection annually, and deciding on how the academy processes and uses biometric data.
- **Trust Data Protection Officer (DPO)**: Responsible for monitoring the academy's compliance with data protection legislation in relation to the use of biometric data, identifying additional risks associated with using automated biometric technology by conducting a DPIA, and being the first point of contact for the ICO and for individuals whose data is processed by the academy and connected third parties.

Data Protection Principles

The academy will process all personal data, including biometric data, in accordance with the key principles set out in the UK GDPR. The academy will 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.
- 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.

As the data controller, the academy will be responsible for being able to demonstrate its compliance with the provisions outlined above. Information will be included in the academy's privacy notices explaining how biometric data is to be processed and stored, including the rights available to individuals in respect of the processing.

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.

- Be reviewed frequently and kept updated.

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 academy 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 academy will adhere to any advice from the ICO. Each DPIA will be treated as a 'living' document to help manage and review the risks of the processing of the biometric data and the measures put in place on an ongoing basis. DPIAs will be reviewed annually or in response to any changes.

Notification and Consent

Consent requirements for biometric information are imposed by section 26 of the Protection of Freedoms Act 2012. Where the academy uses learners' biometric data as part of an automated biometric recognition system (e.g. using learners' fingerprints to receive school dinners instead of paying with cash or a PIN), 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 learners' biometric data, the academy will send learners' parents a Parental Notification and Consent Form for the use of Biometric Data. Written consent will be sought from at least one parent of the learner before the academy collects or uses a learner's biometric data. The name and contact details of learners' parents will be taken from the academy's admission register. Where the name of only one parent 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 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 learner requires that a particular parent is not contacted, e.g. where a learner has been separated from an abusive parent who must not be informed of the learner's whereabouts.
- It is otherwise not reasonably practicable for a particular parent to be notified or for their consent to be obtained.

Where neither parent of a learner can be notified for any of the reasons set out above, consent will be sought from the following individuals or agencies as appropriate:

- If a learner 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 learner and written consent will be obtained from at least one carer before the learner's biometric data can be processed.

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.
- How the data will be stored.
- The parent's and the learner's right to refuse or withdraw their consent.
- The academy's duty to provide reasonable alternative arrangements for those learners whose information cannot be processed.

The academy will not process the biometric data of a learner under the age of 18 in the following circumstances:

- The learner (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.

Parents and learners will be made aware that they can object to participation in the academy's biometric systems or withdraw their consent at any time, and that if they do this, the academy will provide them with an alternative method of accessing the relevant services. Learners will be informed that they can object or refuse to allow their biometric data to be collected and used via letter. The steps taken by the academy to inform learners will take account of their age and level of understanding. Parents will also be informed of their child's right to object and will be encouraged to discuss this with their child.

Where a learner or their parents object, any biometric data relating to the learner that has already been captured will be deleted. If a learner objects or refuses to participate, or to continue to participate, in activities that involve the processing of their biometric data, the academy will ensure that the learner's biometric data is not taken or used as part of a biometric recognition system, irrespective of any consent given by the learner's parent.

Where staff members or other adults use the academy's biometric systems, consent will be obtained from them before they use the system. Staff and other adults can object to taking part in the academy's biometric systems 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 academy's biometric systems.

Alternative Arrangements

Parents, learners, staff members, and other relevant adults have the right to not take part in the academy's biometric systems. Where an individual objects to taking part in the academy's biometric systems, reasonable alternative arrangements will be provided that allow the individual to access the relevant service, e.g. where a biometric system uses learners' fingerprints to pay for school meals, the learner will be able to use cash for the transaction instead. 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 or the learner's parents, where relevant.

Data Retention

Biometric data will be managed and retained in line with the Trust's Data Protection Policy. The academy will only store and process biometric information for the purpose for which it was originally obtained and consent provides. If an individual, including a learner's parent, where relevant, withdraws their consent for their or their child's biometric data to be processed, it will be erased from the academy's system.

Security Measures

The outcome of the DPIA will be used to identify the security measures that will be put in place to protect any unlawful and/or unauthorised access to the biometric data stored by the academy. Biometric data will not be unlawfully disclosed to third parties. These security measures and the process that will be followed if there is a breach to the academy's biometric systems are outlined in the academy's Cyber-security Policy.

Monitoring and Review

The governing board will review this policy on an annual basis. Any changes made to this policy will be communicated to all staff, parents, and learners.

Appendices:

Examples of communications to Parents/Carers

Parental Notification and Consent Form for the Use of Biometric Data

[The following is suggested text for a notification letter and consent form to parents. You should adapt this text in line with your academy's specific biometric systems.]

Address line one Address line two Town County Postcode Date

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

Dear parent,

I am writing to notify you of the 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 learners' fingerprints instead of by 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. their fingerprint. The 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 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 using 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 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 academies when using personal information, such as biometric information, about learners for the purposes of an automated biometric recognition system. For example:

- The academy will not use the information for any purpose other than those for which it was originally obtained and made known to the parent (i.e. as stated above).
- The academy will ensure that the information is stored securely.
- The academy will tell you what it intends to do with the information.

- Unless the law allows it, the academy will not disclose personal information to another person or body.

Please note, the 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 or objecting to the use of biometric information

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

Consent given by one parent will be overridden if another parent 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 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 – their objection does not need to be in writing. We would appreciate if you could discuss this with your child and explain to them that they can object if they want to.

The academy is happy to answer any questions you or your child may have – please contact the DPO on [contact details] with any questions.

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

Please note that, when your child leaves the academy or ceases to use the biometric system, their biometric information will be securely erased in line with the academy's Records Management Policy.

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 academy 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 academy to collect and use the following biometric information relating to your child: [Insert the biometric information the academy intends to collect and use.]

This biometric information will be used by the 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 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 that have provided consent

Please confirm that you have read and understood the following terms:

- I authorise the academy to use my child's biometric information for the purpose specified above until either they leave the 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 [address].
- I understand that once my child ceases to use the biometric system, the academy will securely delete my child's biometric information.

I confirm that I have read and understood the terms above.

For all parents

Name of child: Name of parent: Signature: Date:

Please return this form to the academy office by [date].