Amber Valley & Erewash Support Centre

Biometric Data Policy

Written by:	Janine Dix	**Date:** 05/12/2020
Last reviewed on:	05/12/2020	
Next review due by:	05/12/2021	
Approved by:	Governing Body	
Version:	1	

The Amber valley and Erewash Support Centre is committed to protecting the personal data of all its pupils and staff, this includes any biometric data we collect and process. **We do not currently collect or process biometric data and do not use such a system in our academy.**

However, if we are to consider this in the future then we would store and process data in accordance with relevant legislation and guidance to ensure the data and the rights of individuals are protected.

This policy outlines the procedures that academies should follow when collecting and processing biometric data and emphasises our awareness of such legislation.

BIOMETRIC INFORMATION AND THE 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 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 pupils/staff biometric data, e.g. taking measurements from a fingerprint via a fingerprint scanner.

Storing pupils/staff biometric information on a database - using pupils/staff 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.

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 Headteacher is responsible for reviewing this policy on an annual basis and for ensuring the provisions in this policy are implemented consistently if a biometric data system is used in the academy.

The data protection officer (DPO) is responsible for the monitoring of the academy's compliance with data protection legislation in relation to the use of any biometric data and advising on when it is necessary to undertake a data protection impact assessment (DPIA) in relation to the academy's biometric system. The DPO is also the first point of contact for the ICO and for individuals whose data is processed by the academy and connected third parties.

The Governing Body will ensure that the academy complies with the appropriate legislation if using a biometric data system. The policy will be approved by the Governing Body annually.

DATA PROTECTION IMPACT ASSESSMENTS (DPIAS)

Prior to processing biometric data or implementing a system that involves processing biometric data, academies should ensure that a DPIA is carried out. The DPO should oversee and monitor the process of carrying out the DPIA. The DPIA should:

- 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 should be considered. If a high risk is identified that cannot be mitigated, the DPO should 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. An academy should adhere to any advice from the ICO.

PROVIDING CONSENT/OBJECTING

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 is imposed by section 26 of the Protection of Freedoms Act 2012. Where an academy uses pupils and staff biometric data as part of an automated biometric recognition system (e.g. using pupils' fingerprints to receive academy dinners instead of paying with cash), an academy should comply with the requirements of the Protection of Freedoms Act 2012.

Written consent should be sought from at least one parent of the pupil before an academy collects or uses a pupil's biometric data. The name and contact details of the pupil's parents should be taken from an academy's admission register. Where the name of only one parent is included on the admissions register, the Headteacher should consider whether any reasonable steps can or should be taken to ascertain the details of the other parent. An 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 or if the parent lacks the mental capacity to object or consent. One contact is also acceptable if the welfare of the pupil requires that a particular parent 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 to be notified or for their consent to be obtained.

Where neither parent of a pupil can be notified for any of the reasons, consent should 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 should be notified and their written consent obtained.
- If the above does not apply, then notification should be sent to all those caring for the pupil and written consent obtained from at least one carer before the pupil'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
- The parent's 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

An 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

Parents and pupils can object to participation in an academy's biometric system or withdraw their consent at any time. Where this happens, any biometric data relating to the pupil that has already been captured should 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, an academy should 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.

Where staff members or other adults use an academy's biometric system, consent should be obtained from them before they use the system.

Staff and other adults can object to taking part in an academy's biometric system and can withdraw their consent at any time. Where this happens, any biometric data relating to the individual that has already been captured should be deleted.

Alternative arrangements should be provided to any individual that does not consent to take part in an academy's biometric system.

POSSIBLE ALTERNATIVE ARRANGEMENTS

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

Alternative arrangements would 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, where relevant).

DATA RETENTION

Biometric data should be managed and retained in line with the academy's Records Management Policy.

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

MONITORING AND REVIEW

The Headteacher will review this policy on an annual basis.

If AVESC begin to use a biometric data system in the future then this policy will be made available to all staff, parents, pupils on the academy website.

This policy will be reviewed by the Governing Body for approval annually.

FURTHER INFORMATION AND GUIDANCE

This can be found via the following links:

Department for Education's 'Protection of Biometric Information of Children in Schools – Advice for proprietors, governing bodies, head teachers, principals and school staff:

https://www.gov.uk/government/publications/protection-of-biometric-information-ofchildren-in-schools

ICO guidance on data protection for education establishments:

https://ico.org.uk/for-organisations/in-your-sector/education/