



EFAT Protection of Biometric Information of Children Policy

Date of Issue: 1st November 2020

Next Review Date: 1st November 2021

EFAT Protection of Biometric Information of Children Policy

Contents

1. Purpose of the Policy
2. Biometric Information and How it Should be Used
3. Roles and Responsibilities
4. Data Protection Principles
5. Providing/withdrawing your Consent
6. Data Retention
7. Further Information & Guidance

Policy Cover Note

Title of the Policy	Protection of Biometric Information of Children Policy
Summary/Reason for bringing to Bord for Approval	New Statutory Policy
Statutory Requirement	Yes
Decisions to be made / recommendation on options	Approval required
Name of the author	Maria Neary
Date written	November 2020
Date for Review	November 2021
Policy/Procedure to be published on the trust website	Yes
Policy/procedure to be published on the Academy/Primary website	Yes
Amendments/Updates	

1. Purpose of the Policy

Essa Foundation Academies 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.

2. Biometric Information and How it Should be Used

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'

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.

3. Roles and Responsibilities

The CEO is responsible for:

- Reviewing this policy on an annual basis.

The Principals are responsible for:

- Ensuring the provisions in this policy are implemented consistently.

The Data Protection Officer (DPO) is responsible for:

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

4. Data Protection Principles

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

The Trust 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.
- As the data controller, the Trust is responsible for being able to demonstrate its compliance with the provisions outlined above

5. Providing/withdrawing your 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 is imposed by section 26 of the Protection of Freedoms Act 2012.

Where the Trust uses pupils and staff 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 Trust will comply with the requirements of the Protection of Freedoms Act 2012.

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

The name and contact details of the pupil's parents will be taken from the Academy's MIS system.

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.

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 Trust's duty to provide reasonable alternative arrangements for those pupils whose information cannot be processed

The Trust 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 the Trust'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.

If a pupil objects or refuses to participate, or to continue to participate, in activities that involve the processing of their biometric data, the Trust 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).

Alternative arrangements will be provided to any individual that does not consent to take part in the Trust's biometric system(s). 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, where relevant).

6. Data Retention

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

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

7. Further Information & 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-of-children-in-schools>

ICO guidance on data protection for education establishments: <https://ico.org.uk/for-organisations/in-your-sector/education/>