

PROTECTION OF BIOMETRIC INFORMATION POLICY

Approving Body	Trust
Date of Last Review	May 2023
Statutory (Y/N)	Y
Responsible Officer	BMAT CEO for and on behalf of the Trust

I. INTRODUCTION – LEGISLATION AND DEFINITIONS

1. This Policy forms part of BMAT’s commitment to protecting the personal data of its students and staff. This Policy outlines the procedures that are in place relating to the processing of biometric data.
2. This Policy has been drafted in line with:
 - a. Relevant legislation, including the Data Protection Act 2018, the UK GDPR is the UK General Data Protection Regulation (GDPR) 2021 and the Protection of Freedoms Act 2012; and guidance from the Department for Education (DfE), “Protection of Biometric Information of Children in Schools and Colleges”.
 - b. BMAT’s [Data Protection Policy](#).
3. Definitions:
 - a. “Biometric data” means personal information about an individual’s physical or behavioural characteristics that can be used to identify them, including their fingerprints, facial shape, retina and iris patterns, and hand measurements. Biometric data is classed as “special category data” or “sensitive personal data” under the Data Protection Act 2018.
 - b. “Automated biometric recognition system” means 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.
 - c. “Processing biometric data”: Processing biometric data includes obtaining, recording, holding 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 it records, stores, accesses and compares biometric data.

II. ROLES AND RESPONSIBILITIES

4. The BMAT Data team and the BMAT Data Protection Officer (DPO), are responsible for the day to day implementation of this Policy and our Data Protection Policy, with accountability to the BMAT Trust Executive. This responsibility includes monitoring compliance with data protection requirements, advising on data protection impact assessments and being the first point of contact for the Information Commissioner’s Office (ICO). in relation to the use of biometric data.
5. The BMAT Trust Executive, which includes all BMAT School Principals, is responsible for the oversight and implementation of this Policy, under the leadership of the BMAT CEO with accountability to the Board of Trustees.

III. PROTECTION PRINCIPLES

6. BMAT processes all personal data, including biometric data, in accordance with the key principles set out in the Data Protection Act 2018, which are reflected in the [BMAT Data Protection Policy](#).
7. BMAT ensures that all biometric data is:
 - a. Processed lawfully, fairly and in a transparent manner.
 - b. Only collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes.
 - c. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
 - d. Accurate and, where necessary, kept up-to-date, and that reasonable steps are taken to ensure inaccurate information is rectified or erased.
 - e. Kept in a form which permits the identification of individuals for no longer than is necessary for the purposes for which the personal data are processed.
 - f. Processed in a way 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.
8. As the data controller, BMAT is responsible for being able to demonstrate its compliance with the provisions outlined above.
9. Data protection impact assessments (DPIAs)
 - a. Prior to processing biometric data or implementing a system that involves processing biometric data, a DPIA will be carried out.
 - b. The DPO will oversee and monitor the process of carrying out the DPIA.
 - c. The DPIA will outline the form of data processing, assess necessity, proportionality and compliance, identify risks to individuals and identify measures to mitigate those risks.
 - d. The ICO may be consulted as part of the DPIA process, for example to determine if a specific form of data processing is compliant.

IV. THE USE OF BIOMETRIC INFORMATION BY BMAT AND ITS SCHOOLS

10. BMAT uses student and employee fingerprint data, as part of 'Parent Pay' - an automated biometric recognition system, which enables us to operate a cashless system, in the interests of efficiency and safety on BMAT premises.

11. BMAT's use of biometric data complies with the Protection of Freedoms Act 2012.

12. BMAT Students:

- a. BMAT will not process the biometric data of its students if the student objects and if a parent or carer has refused, withdrawn or not given consent
- b. Parents/carers are notified before their child first takes part in the Parent Pay biometric recognition system;
- c. The name and contact of parents/carers will be taken from the admission register/student records system;
- d. Written consent is obtained from at least one parent/carers before we take and process biometric data from a student;
- e. If the details of only one parent/carers are included in its records, BMAT will consider whether any reasonable steps ought to be taken to find the details of the other parent/carers and contact them.
- f. BMAT is not obliged to seek the consent of a particular parent or carer if it is satisfied that their whereabouts are unknown, they lack the capacity to consent, the welfare of the child requires that a particular parent is not contacted or it is not otherwise practicable for consent to be obtained.
- g. If a child is "looked after" by the local authority or a voluntary organisation, BMAT will seek consent from an appropriate contact at that organisation.
- h. Requests for consent will include details about the type of biometric information that will be used, how it will be used, the right to refuse or withdraw consent and BMAT's duty to provide reasonable alternative arrangements if consent is refused or withdrawn.
- i. Parents/carers and students may choose not to provide their biometric data for Parent Pay.
- j. When this right is exercised, BMAT will make arrangements for the student in question to access the relevant services. For example, parents/carers can pay for school lunches in advance by cheque or transfer.
- k. Parents/carers and students can withdraw consent to participate in Parent Pay at any time, by submitting a written request to the BMAT DPO at dpo@beaconacademytrust.co.uk or 'Data Protection Officer, The Beacon Multi-Academy Trust, Ilford, IG4 5LP.
- l. BMAT employees who receive such a request must not respond to it and must forward it to the BMAT DPO immediately;
- m. As required by law, if a student refuses (verbally or non-verbally) to participate, or continue to participate, in Parent Pay, their biometric data will not be processed, irrespective of parental/carers consent;
- n. If consent is withdrawn, any biometric data already captured will be deleted and erased from BMAT's records.

- o. Otherwise, biometric data will be stored and retained in line with the BMAT Data Retention Schedule, which is annexed to the [BMAT Data Protection Policy](#) or available on request from the DPO.

13. BMAT employees:

- a. Consent will also be obtained from employees before processing their biometric data for Parent Pay.
- b. The above provisions, on the individual data subject's right to refuse or withdraw consent and be provided with alternative means of payment, apply.
- c. Biometric data will be stored and retained in line with the BMAT Data Retention Schedule, which is annexed to the [BMAT Data Protection Policy](#) or available on request from the DPO.