East Midlands Academy Trust

Biometric Data Protection Policy 2022/2024

'Every child deserves to be the best they can be'

Scope: East Midlands Academy Trust & Academies within the Trust	
Version: V2	**Filename:** EMAT Biometric Data Protection Policy
Approval: July 2022	**Next Review: July 2024** *This Policy will be reviewed by the Trust Board every two years (FHRE)*
Owner: East Midlands Academy Trust Board of Trustees	**Union Status:** Not Applicable

Policy type:	
Statutory	Replaces Academy's current policy

RevisionDate	Revisor	Description of Revision
July 2022 – V2	M Juan	Policy review – No Changes
July 2020 – v1	M Juan	New EMAT Biometric Data Protection Policy issued to all schools

EMAT Biometric Data Protection Policy

1. Introduction

We believe this policy should be a working document that is fit for purpose, represents the Trust's ethos, enables consistency and quality across the Trust and is related to the following legislation:

- Equality Act 2010
- Education Act 2011
- Protection of Freedoms Act 2012
- Data Protection Act 2018

The following documentation is also related to this policy:

- Protection of biometric information of children in schools and colleges: Advice for proprietors, governing bodies, head teachers, principals and school and college staff (DfE 2018)
- Equality Act 2010: Advice for Schools (DfE)
- Race Disparity Audit - Summary Findings from the Ethnicity Facts and Figures Website (Cabinet Office)
- Data Protection: a toolkit for schools (DfE)

East Midlands Academy Trust has a duty that when using automated biometric recognition systems, to have in place arrangements to notify parents and obtain their consent. We are aware that there are no circumstances in which we can lawfully process a pupil's biometric data without having notified each parent of a child and received the necessary consent.

The Trust understand that biometric data means 'personal information about an individual's physical or behavioural characteristics that can be used to identify that person; this can include their fingerprints, facial shape, retina and iris patterns, and hand measurements'.

The Trust is aware that 'the Information Commissioner considers all biometric information to be personal data as defined by the Data Protection Act 1998; this means that it must be obtained, used and stored in accordance with that Act'.

The Trust understand the 'Protection of Freedoms Act includes provisions which relate to the use of biometric data in schools and colleges when used as part of an automated biometric recognition system. These provisions are in addition to the requirements of the Data Protection Act 1998'.

The Trust recognise that biometric technology has been used in the UK since the beginning of the 21st century by addressing truancy, replacing library cards, and to charge for meals. The use of electronic fingerprinting systems has raised privacy concerns because of the creation of databases that would progressively include the entire population.

The Trust realise that:

- 'automated biometric recognition systems uses technology 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';
- 'biometric recognition systems can use many kinds of physical or behavioural characteristics such as those listed in section 1 of the 'What is biometric data' section above'

The Trust acknowledges that:

- 'Processing' of biometric information includes obtaining, recording or holding the data or carrying out any operation or set of operations on the data including (but not limited to) disclosing it, deleting it, organising it or altering it. An automated biometric recognition system processes data when:
  - o recording pupils' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner;
  - o storing pupils' biometric information on a database system; or
  - o using that data as part of an electronic process, for example, by comparing it with biometric information stored on a database in order to identify or recognise pupils

  (Protection of biometric information of children in schools and colleges: (DfE)

The Trust has a responsibility to ensure equality permeates in to all aspects of school life and that everyone is treated equally irrespective of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation. Everyone connected with the Trust should feel safe, secure, valued and of equal worth.

We acknowledge the findings of the Race Disparity Audit that clearly shows how people of different ethnicities are treated across the public services of health, education, employment and the criminal justice system. The educational section of the audit that covers: differences by region; attainment and economic disadvantage; exclusions and abuse; and destinations, has a significant importance for the strategic planning of this school.

We believe it is essential that this policy clearly identifies and outlines the roles and responsibilities of all those involved in the procedures and arrangements that is connected with this policy.

2. Aims

- To treat pupils' biometric data collected with appropriate care and to comply with the data protection principles as set out in the Data Protection Act 1998.
- To ensure compliance with all relevant legislation connected to this policy.

3. Responsibility for the Policy and Procedure

Role of the Trust Board

The Trust Board has:

- appointed a Data Protection Officer;
- delegated powers and responsibilities to the Head of Shared Services, Academy Headteachers and to ensure all Trust personnel and stakeholders are aware of and comply with this policy;
- responsibility for ensuring:

  o full compliance with all statutory responsibilities; including equalities legislation
  o funding is in place to support this policy;
  o this policy and all policies are maintained and updated regularly;
  o all policies are made available to parents;
  o the nomination of a designated Equalities governor to ensure that appropriate action will be taken to deal with all prejudice related incidents or incidents which are a breach of this policy;

Role of the Local Advisory Board (LAB)

The LAB has:

- appointed a link governor to:

  o visit the Trust regularly;
  o work closely with Headteachers, the Head of Shared Services and the DPO
  o ensure this policy and other linked policies are up to date;
  o ensure that everyone connected with the school is aware of this policy;
  o attend training related to this policy;
  o report to the Governing Body every term;
  o annually report to the Governing Body on the success and development of this policy
  o review the effective implementation, monitoring and evaluation of this policy

Role of the Data Protection Officer (DPO)

The Data Protection Officer will:

▪ treat the data collected with appropriate care;
▪ comply with the data protection principles as set out in the Data Protection Act 1998;
▪ when the data is used as part of an automated biometric recognition system comply with the additional requirements in sections 26 to 28 of the Protection of Freedoms Act 2012;
▪ ensure that each parent of a child is notified of the school's intention to use the child's biometric data as part of an automated biometric recognition system;
▪ ensure the written consent of at least one parent will be obtained before the data is taken from a child under the age of 18 and used;
▪ not process the biometric data of a pupil (under 18 years of age) where:

  o the child (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data;

  o no parent has consented in writing to the processing; or

  o a parent has objected in writing to such processing, even if another parent has given written consent.

▪ provide reasonable alternative means of accessing services for those pupils who will not be using an automated biometric recognition system;
▪ store biometric data securely to prevent any unauthorised or unlawful use;
▪ not keep biometric data for longer than it is needed;
▪ must destroy a child's biometric data if a pupil no longer uses the system or when he/she leaves the Trust or where a parent withdraws consent or the child objects;
▪ ensure that biometric data is used only for the purposes for which they are obtained and that such data are not unlawfully disclosed to third parties;
▪ train Trust personnel;
▪ keep up to date documentation of all data protection activities;
▪ work closely with Chief Executive, Head Teachers and nominated governor;
▪ periodically report to the Chief Executive, Headteachers and to the LAB;
▪ annually report to the Trust Board on the success and development of this policy

Role of Headteacher

The Headteacher will:

▪ work in conjunction with the Executive Team to ensure all Trust personnel, pupils and parents are aware of and comply with this policy;
▪ take steps to ensure parents receive full information about the processing of their child's biometric data including:
  o a description of the proposed biometric system;
  o the nature of the data the Trust wishes to process; and
  o the purpose of the processing and how the data will be obtained and used;

- provide pupils with information in a manner that is appropriate to their age and understanding;
- notify both parents of a child whose biometric information the Trust wishes to collect/use but if one parent objects in writing, then the school will not be permitted to take or use that child's biometric data;
- ensure pupils are aware that they have a right to object (this does not have to be writing) and can object to the processing of their biometric data or refuse to take part at any stage;
- in the event that a pupil objects:

    o will not start to process his or her biometric data; or
    o will stop the process if it has already started

- be aware that the Trust is not required by law to consult parents before installing an automated biometric recognition system but will consult with parents and pupils before introducing such a system;
- notify parents and secure consent (either in writing or by verified email) from at least one parent before biometric data is obtained or used for the purposes of such a system;
- be aware that we do not need to renew consent every year as the original consent is valid until such time as it is withdrawn;
- be aware that the original consent can be overridden at any time if another parent objects in writing or if the child objects to the processing;
- understand that when the pupil leaves the Trust his/her biometric data will be securely removed from the system;
- notify and obtain consent from parents when the Trust introduces an additional, different type of automated biometric recognition system;
- inform parents that they have the right to withdraw their consent in writing at any time;
- be aware that the Protection of Freedoms Act covers all systems that record or use physical or behavioural characteristics for the purpose of identification such as palm, iris or face recognition or fingerprints;
- provide reasonable alternative arrangements for pupils who do not use the automated biometric recognition systems;
- ensure pupils who do not participate in the automated biometric recognition system do not suffer any disadvantage from the alternative arrangements;
- ensure that the alternative arrangements do not place any additional burden on parents whose children are not participating in such a system;
- work closely with the link governor and Data Protection Officer;
- provide leadership and vision in respect of equality;
- make effective use of relevant research and information to improve this policy;
- provide guidance, support and training to all staff;
- make effective use of relevant research and information to improve this policy;
- monitor the effectiveness of this policy by speaking with pupils, parents, Trust personnel, and governors;
- annually report to the LAB on the success and development of this policy

Role of Trust Personnel

Trust personnel will:

- comply with all aspects of this policy;
- be aware of all other linked policies

Role of Pupils

Pupils will:

- be aware of and comply with this policy;
- be made aware of their rights

Role of Parents/Carers

Parents/carers will:

- be aware of and comply with this policy;
- work in partnership with the school;
- comply with this policy for the benefit of their children;
- be made aware of their rights

4. Raising Awareness of this Policy

We will raise awareness of this policy via:

- Trust and Academy Handbook/Prospectus;
- Trust and Academy websites;
- Staff Handbook;
- Meetings with Trust personnel;
- Written communications with home such as newsletters;
- Annual report to parents;
- Headteacher reports to the LAB and CEO
- Information displays in the main Academy entrances;
- Text messages
- Email
- Social media

5. Training

All Trust personnel:

- have equal chances of training, career development and promotion;
- receive training on induction which specifically covers:

    o All aspects of this policy
    o Cyber Security
    o Data Protection and the General Data Protection Regulation
    o Management of School Records
    o School Data Retention and School Data Management
    o Vital School Records
    o Equal opportunities
    o Inclusion

- receive periodic training so that they are kept up to date with new information;
- receive equal opportunities training on induction in order to improve their understanding of the Equality Act 2010 and its implications

6. Equality Impact Assessment

Under the Equality Act 2010 we have a duty not to discriminate against people on the basis of their age, disability, gender, gender identity, pregnancy or maternity, race, religion or belief and sexual orientation. This policy has been equality impact assessed and we believe that it is in line with the Equality Act 2010 as it is fair, it does not prioritise or disadvantage any pupil and it helps to promote equality at this school.

7. Monitoring the Implementation and Effectiveness of the Policy

The practical application of this policy will be reviewed annually or when the need arises by the coordinator, the Chief Executive and the nominated governor. A statement of the policy's effectiveness and the necessary recommendations for improvement will be presented to the LAB for further discussion and endorsement.

8. Linked Policies

- Cyber Security
- Data Protection and the General Data Protection Regulation
- Management of School Records
- School Data Retention and School Data Management

East Midlands Academy Trust is a company limited by guarantee registered in England & Wales No. 08149829
Orchard Academy, Shepherdswell Academy, Castle Academy, Hardingstone Academy, Stimpson Avenue Academy,
Prince William School and Northampton International Academy are all business names of the East Midlands Academy Trust.