Protection of Biometric Data Policy

Document control		POLICY LEVEL: Trust / Statutory	
Approved by	Full Trustees	Approved Date	17 March 2022
Portfolio	Data Protection	Next Review	01 March 2023
Published Location	https://www.dartmoormat.org.uk/policies-and-documents.html		
Version Number	Date issued	Author	Update information
1.0	28 Feb 2020	N McDermott	First Published Version
2.0	12 Mar 2021	N McDermott	3.3 role of DPL included at school level.
3.0	03 Mar 2022	J Coundon	'Biometric Information and How it Will be Used', updated Addition of 'Why Biometric Information Will be Used'. 2.1 and 2.2 updated, 'Data Protection Principles' replaced with 'Lawful Basis for Processing Biometric Data, 6.1 & 6.11 removed

Statement of Intent

The Dartmoor Multi Academy Trust is committed to protecting the personal data of all its learners 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. This policy outlines the procedure the academies follow when collecting and processing biometric data.

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.

Within the Dartmoor Multi Academy Trust, we use CRB Cunninghams ID Management software, which uses fingerprint measurements to process cashless catering within our secondary academies only, and in some secondary colleges, to process library management systems. We do not use facial recognition software.

The image taken is a numeric measurement fed into an algorithm to encrypt the data. The actual image is not stored.

Why biometric information is used

- Biometric systems can be faster than using passwords or manual processes.
- Biometrics can be more convenient, as they cannot be lost, misplaced or damaged.
- Biometrics provide additional security as they cannot be stolen or loaned to someone else.

Providing your consent/objecting to the use of biometric data

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

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 following Trust policies:

- Data Protection Policy
- Records Management 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. Within the Dartmoor Multi Academy Trust, we use fingerprints only.

Where biometric data is used for identification purposes, it is considered special category data as defined by the General Data Protection Regulations (GDPR) and Data Protection Act 2018 (DPA).

Dartmoor Multi Academy Trust is registered with the ICO as a data controller and complies with data protection legislation and principles. The school will only use biometric data collected lawfully and with appropriate care.

The Protection of Freedoms Act 2012 includes provisions which relate to the use of biometric data in schools, when it is used as part of an automated biometric recognition system.

These provisions are in addition to the requirements of the Data Protection Act 2018 and are laid out in sections 26 to 28 of the Protection of Freedoms Act 2012.

As the data controller, the school is responsible for being able to demonstrate its compliance with these additional provisions, as outlined above.

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 to recognise or identify the individual. To be recognised, an individual must have been previously subject to "enrolment".

This is the process where samples of biometric data, such as fingerprints, are captured from an individual and stored to allow comparison in the future.

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 learners' biometric data, e.g., taking measurements from a fingerprint via a fingerprint scanner.
- Storing learners' biometric information on a database.
- Using learners' biometric data as part of an electronic process, e.g. by comparing it with biometric information stored on a database to identify or recognise learners.

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 Principal of each school is responsible for ensuring the provisions in this policy are implemented consistently.

The Data Protection Lead (DPL) in each school of DMAT is responsible for:

- Monitoring the school's compliance with data protection legislation in relation to the use of biometric data.

The Trust's Data Protection Officer

- Advising on when it is necessary to undertake a data protection impact assessment (DPIA) in relation to the academy's biometric system(s).
- Being the first point of contact for the ICO and for individuals whose data is processed by the academy and connected third parties.
- 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.

Lawful Basis for Processing Biometric Data

Biometric data is classified as Special Category data under the GDPR and DPA. A lawful basis for processing under Article 9 of GDPR must be identified.

For the purposes of biometrics, the lawful basis is Article 9(2)(a) Explicit Consent.

The consent requirements for biometric information are imposed by section 26 of the Protection of Freedoms Act 2012.

The written consent of at least one parent must be obtained before the data is taken from the child and used (i.e. 'processed'). This applies to all pupils in schools and colleges under the age of 18. In no circumstances will a child's biometric data be processed without written consent.

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. A DPIA has been completed for CRB Cunninghams ID Management.

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.

When assessing levels of risk, the likelihood and the severity of any impact on individuals will be considered. No high risks have been identified for CRB Cunninghams ID Management.

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 DPO 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.

Notification and Consent

Prior to processing a learner's biometric data, the academy will send the parents/ carers a consent form or collect this consent via secure online systems.

Consent will be sought from at least one parent of the learner before the academy collects or uses a learner's biometric data.

Information provided to parents /carers will include information regarding the following:

- How the data will be used
- The parent's and the child'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 can object to participation in the academy's biometric system(s) or withdraw their consent at any time. Where this happens, 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(s).

Learners will be informed that they can object or refuse to allow their biometric data to be collected and used via the consent information.

Where staff members or other adults use the academy's biometric system(s), 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 system(s) 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

Learners and staff have the right to not take part in the academy's biometric system.

Where an individual objects to taking part in the academy's biometric system(s), reasonable alternative arrangements will be provided that allow the individual to access the relevant service, e.g., where a biometric system uses fingerprints to pay for school meals, the person will be able to use a 4-digit PIN instead or by name lookup.

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 learner's parents, where relevant).

Data Retention

Biometric data will be managed and retained in line with the Trust's Records Management Policy.
If an individual (or a learner's parent, where relevant) withdraws their consent for their/their child's biometric data to be processed, it will be erased from the academy's system.

Breaches

There are appropriate and robust security measures in place to protect the biometric data held by the academy. These measures are detailed in the DPIA.

Any breach to the college biometric system will be dealt with by the Trust DPO.