# Protection of Biometric Data Policy

| Document control | | | POLICY LEVEL: Trust / Statutory | |
|---|---|---|---|---|
| Approved by | Trust Board | | Approved Date | 14 September |
| Portfolio | Data Protection | | Next Review | July 2024 |
| Published Location | Intranet and website | | | |
| **Version** | **Date** | **Author** | **Update information** | |
| 1.0 | 28 Feb 2020 | NMD | First Published Version | |
| 2.0 | 12 Mar 2021 | NMD | 3.3 role of DPL included at school level. | |
| 3.0 | 03 Mar 2022 | JC | 'Biometric Information and How it Will be Used', updated Addition of 'Why Biometric Information Will be Used'.<br>2.1 and 2.2 updated, 'Data Protection Principles' replaced with 'Lawful Basis for Processing Biometric Data, 6.1 & 6.11 removed | |
| 4.0 | July 2023 | MeG | New policy based on template designed by DPO and includes Spring 23 update. 12.10 additional reference to ICO case study on facial recognition. 12.16 DfE guidance date updated | |

This document will be reviewed annually and sooner when significant changes are made to the law.

Guidance from the Department for Education about school policies can be found here: https://www.gov.uk/government/publications/statutory-policies-for-schools-and-academy-trusts/statutory-policies-for-schools-and-academy-trusts

# Protection of Biometric Data Policy

## Contents


1. Introduction ..... 2
2. Notification and Consultation ..... 3
3. Biometric Information Definition ..... 3
4. Why Biometric Information Is Used ..... 3
5. Automated Biometric Recognition Systems ..... 3
6. Roles and Responsibilities ..... 3
7. Data Protection Impact Assessments ..... 4
8. Biometric Data Classification ..... 4
9. Data Processing ..... 4
10. Lawful Basis for Processing Biometrics Data ..... 5
11. Consent Requirements ..... 5
    11.1 Staff ..... 5
    11.2 Pupils ..... 5
12. Consent limitations ..... 6
13. Alternative arrangements ..... 6
14. Data Security ..... 6
15. Data Retention ..... 6
16. Relevant Legislation ..... 7


# 1. Introduction

Dartmoor Multi Academy Trust (the Trust) wishes to use biometric information as part of an automated (i.e. electronically-operated) recognition system.

This is for the purpose of allowing cashless catering payments and (where appropriate devices are installed) allowing students to check account balance. This information is referred to as 'biometric information' (see next paragraph).

The Trust intends to enrol pupils by capturing their fingerprint which will be stored on a physically and cryptographically secure server on site.

## 2. Notification and Consultation

The Trust will 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.

Notification will be in line with the requirements detailed in the "Protection of biometric information of children in schools and colleges".

## 3. Biometric Information Definition

Biometric data is personal information about an individual's physical or behavioural characteristics that can be used to identify that person.

This includes, but is not limited to, their fingerprints, facial shape, retina and iris patterns, and hand measurements.

## 4. Why Biometric Information Is Used

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

## 5. Automated Biometric Recognition Systems

An automated biometric recognition system 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.

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.

Further information can be found at: https://www.ncsc.gov.uk/collection/biometrics

## 6. Roles and Responsibilities

1. The Trust Board are responsible for reviewing this policy annually.

2. The Principal is responsible for ensuring this policy is communicated to all relevant stakeholders and the provisions in this policy are implemented consistently.

3. The Data Protection Officer (DPO) is responsible for advising of any necessary data protection impact assessment (DPIA) in relation to biometric system(s).
   The DPO is also the first point of contact for the ICO.

## 7. Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) must be carried out before any biometric data system is purchased or implemented, assessing any risks to data subjects and the measures the School will take to minimise the risks. This is in line with UK GDPR legal requirements.

The DPO will oversee and monitor the process of carrying out the DPIA, but the decision to purchase and implement a system will be taken by the Trust Board.

When assessing levels of risk, the likelihood and the severity of any impact on individuals will be considered prior to the processing of any biometric data.

## 8. Biometric Data Classification

Personal data which is more sensitive, and so needs more protection, is classed as special category data.

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

Each school within the 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.

## 9. Data Processing

'Processing' of biometric information includes obtaining, recording, storing, disclosing, analysing, using, deleting, organising or modifying it.

An automated biometric recognition system processes data when:

1. Biometric data is recorded, for example, capturing a fingerprint via a fingerprint scanner.
2. Storing biometric information on a database or as part of a purchased system.
3. Using the recorded biometric data as part of an electronic process, to identify or recognise individuals.

## 10. Lawful Basis for Processing Biometrics Data

Biometric data is classified as Special Category data under the GDPR and DPA 2018. Therefore, a lawful basis for processing under Article 9 of the UK GDPR must be identified by the school, in addition to a lawful basis under Article 6 of the UK GDPR.

For the purposes of processing biometrics data of children in a school setting, the lawful basis is Explicit Consent (Article 9(2)(a)).

This requirement for consent for processing children's biometric information is 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.

In addition, even if a parent consents, the child may object to the processing of their biometric data or refuse to cooperate with the biometric data collection or use. The child's objection/refusal takes precedent over the parents' consent.

Measures must be put in place to ensure children can still access all services, etc. that the biometric data processing is designed to allow access to, even if they do not have their biometric data processed.

Further information can be found in the ICO guidance on data protection for education establishments. In relation to Facial Recognition Technology, the ICO have published a case study which sets out useful guidance on the data protection implications of such processing.

## 11. Consent Requirements

### 11.1 Staff

Schools are obliged to obtain consent for the processing of any biometric information, whether for adults and children.

Consent will be sought from staff members or other adult stakeholders prior to the processing of their biometric data.

Staff and other adults can object to the collection of their biometric data and can withdraw their consent at any time. If consent is withdrawn any biometric data relating to the individual that has already been captured will be deleted.

### 11.2 Pupils

Written consent will be sought from at least one parent of any child or young person under the age of 18.

Consent given by one parent will be overridden if the other parent objects in writing to the use of their child's biometric information. Objections should be addressed to the Principal.

Parental consent can also be overridden by the child.

For looked after pupils, the LA will be notified and notification will also be sent to all those caring for the pupil. Written consent will be obtained from at least one carer before the pupil's biometric data can be processed.

## 12. Consent limitations

Where the school only holds contact information for only one parent, staff will consider whether any reasonable steps can or should be taken to ascertain the details of the other parent.

The school does not need to notify a particular parent or seek their consent if it is satisfied that:

- The parent cannot be found, after reasonable steps have been taken
- The parent lacks the mental capacity to object or consent.
- Welfare or safeguarding concerns require that a particular parent is not contacted.
- It is not practicable for a particular parent to be contacted.

## 13. Alternative arrangements

Alternative arrangements will be provided to any individual that does not consent to the processing of their biometric information.

Where an individual objects to taking part in the School's biometric data processing system(s), reasonable alternative arrangements will be provided that allow the individual to access the relevant service.

Catering payments may be made by students by giving their name at checkout. Staff will look up the individual and compare the student with the photograph synced from the MIS system. Where no photo permissions have been given the student will be issued with a PIN. Account balance checks can be carried out by speaking to the appropriate administrative staff.

The school will ensure alternative arrangements do not put an individual (or the parents of pupils) at any disadvantage, create access difficulties or result in additional burdens.

## 14. Data Security

Biometric information used to identify a person is based upon an image taken of their fingerprint. The image taken is a numeric measurement fed into an algorithm to encrypt the data. The actual image is not stored.

The system is one directional, meaning that it is impossible to reverse the process to recreate a fingerprint/facial likeness.

## 15. Data Retention

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

Where consent is withdrawn by an individual, or the parent of a pupil under 18, biometric data relating to that individual will be erased from the system.

Where staff or pupils cease to use the biometric system, their biometric information will be securely erased.

## 16. Relevant Legislation

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
- UK General Data Protection Regulation (UK GDPR)
- DfE (2022) 'Protection of biometric information of children in schools and colleges'

This policy operates in conjunction with the following school policies:

- Data Protection Policy
- Information Security Policy