



# Protection of Biometric Information Policy

| Review Date    | Reviewer | Adopted       | Implementation |
|----------------|----------|---------------|----------------|
|                | J Barker | 17 March 2021 | 18 March 2021  |
| September 2023 | J Barker |               |                |
|                |          |               |                |
|                |          |               |                |
|                |          |               |                |

## REVISION HISTORY

| Issue No | Date       | Description |
|----------|------------|-------------|
| 1        | March 2021 | New Policy  |
|          |            |             |
|          |            |             |
|          |            |             |
|          |            |             |
|          |            |             |
|          |            |             |
|          |            |             |
|          |            |             |
|          |            |             |
|          |            |             |
|          |            |             |
|          |            |             |
|          |            |             |

|           |            |                                 |                   |
|-----------|------------|---------------------------------|-------------------|
| Issue No: | 1          | Quality Document Type:          | Policy            |
| Date:     | 01/04/2021 | Ref:                            | TRUST/GDPR/PBIFSP |
|           |            | Originator of this document is: | J Barker          |

|    | <b>Contents</b>                    | <b>Page No.</b> |
|----|------------------------------------|-----------------|
| 1. | Introduction                       | 4               |
| 2. | Links to other policies            | 4               |
| 3. | Scope                              | 4               |
| 4. | Definitions                        | 4               |
| 5. | Data Protection principles         | 5               |
| 6. | Data Protection Impact Assessments | 5               |
| 7. | Parental Consent and Notification  | 6               |
| 8. | Data retention                     | 7               |
| 9. | Breaches                           | 7               |

## 1 Introduction

The Protection of Biometric Information Policy outlines the procedure the North East Learning Trust follows when collecting and processing biometric data. The Information Commissioner considers all biometric information to be personal data as defined by the General Data Protection Regulation; this means that it must be obtained, used, and stored in accordance with that Regulation. The Protection of Freedoms Act 2012 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 General Data Protection Regulation.

## 2. Links to other policies

This policy should be read in conjunction with the following Trust and Academy policies:

- Acceptable Use
- Data Protection
- Data Retention

## 3. Scope

This policy applies to all Trust employees and student/pupils attending an Academy that is part of the North East Learning Trust.

## 4. 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' biometric data, e.g. taking measurements from a fingerprint via a fingerprint scanner.
- Storing pupils' biometric information on a database.
- Using pupils' 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.

|           |            |                                 |                   |
|-----------|------------|---------------------------------|-------------------|
| Issue No: | 1          | Quality Document Type:          | Policy            |
| Date:     | 01/04/2021 | Ref:                            | TRUST/GDPR/PBIFSP |
|           |            | Originator of this document is: | J Barker          |

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.

## 5. 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.

## 6. 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. The DPO will oversee and monitor the process of carrying out the DPIA with the Director of IT.

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. If

|           |            |                                 |                   |
|-----------|------------|---------------------------------|-------------------|
| Issue No: | 1          | Quality Document Type:          | Policy            |
| Date:     | 01/04/2021 | Ref:                            | TRUST/GDPR/PBIFSP |
|           |            | Originator of this document is: | J Barker          |

a high risk is identified that cannot be mitigated, the DPO will consult the ICO before the processing of the biometric data begins. The Trust will adhere to any advice from the ICO.

## 7. Parental Consent and Notification

The Trust is aware of 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.

All Academies within the Trust will ensure that the parent/carer of each pupil/student is informed of the intention to use the child's biometric data as part of an automated biometric recognition system. The written consent of the parent/carer or the child, where the child is deemed to have the capacity to consent, will be obtained before the data is taken from the child and used (i.e. '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 Academy's duty to provide reasonable alternative arrangements for those pupils whose information cannot be processed.

In no circumstances will an Academy process a child's biometric data without written consent.

Primary Academies within the Trust will not process the biometric data of a pupil aged 4 -11 years old in the following circumstances:

- 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

Secondary Academies with the Trust will not process the biometric data of a student aged 12 to 18 years old in the following circumstances:

- The child (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data.
- A parent or student has not consented in writing to the processing.
- A parent or student has objected in writing to such processing, even if another parent has given written consent.

The original written consent is valid until such time as it is withdrawn. However, it can be overridden, at any time either parent/carer or the child themselves objects to the processing (subject to the objection being in writing).

|           |            |                                 |                   |
|-----------|------------|---------------------------------|-------------------|
| Issue No: | 1          | Quality Document Type:          | Policy            |
| Date:     | 01/04/2021 | Ref:                            | TRUST/GDPR/PBIFSP |
|           |            | Originator of this document is: | J Barker          |

Staff and other adults can object to taking part in the school'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 will be provided to any individual that does not consent to take part in the school's biometric systems

## 8. Data Retention

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

## 9. Breaches

There are appropriate and robust security measures in place to protect the biometric data held by the school. These measures are detailed in the Data Protection Policy. Any breach to the Academy biometric systems will be dealt with in accordance with the policy.

|           |            |                                 |                   |
|-----------|------------|---------------------------------|-------------------|
| Issue No: | 1          | Quality Document Type:          | Policy            |
| Date:     | 01/04/2021 | Ref:                            | TRUST/GDPR/PBIFSP |
|           |            | Originator of this document is: | J Barker          |