Nene Education Trust
Protection of Biometric Data Policy
Policy number 41

Key Manager:	**Trust GDPR Lead**
Ratified by Trustees:	
Review Dates:	**Summer 2023**
Location of Policy:	**Trust Intranet**
Access to Policy:	**Open**
Policy Context:	**This Policy applies to all staff and pupils of the Nene Education Trust.**

Revision History

Revision Date	Description	Sections Affected	Revised By	Approved By
June 2020	New policy	All sections	Governance Manager and Trust DPO	CEO
Summer 2021	No changes			
Summer 2022	Replaced 'Governance Manager' with 'Trust GDPR Lead'	All sections	Trust GDPR Lead and DPO	

Statement of intent

Nene Education 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 Trust and its schools will follow when collecting and processing biometric data (currently only used within Manor School).

Biometric information and how it will be used

Biometric information are details about a person's physical or behavioural characteristics that can be used to identify them, e.g. their fingerprint.

The data collected will be used as part of an automated biometric recognition system.

This system will take measurements of the biometric information specified above (fingerprint) and convert these measurements into a template to be stored on the

system. An image of data is not stored. The template (i.e. the measurements) will be used to permit payment at the canteen till and for the loan of library books from the school Learning Resource Centre.

Providing your consent/objecting to the use of biometric data

Parents/carers/staff who object to finger print data being retained, agree to being issued with a 4-digit pin code and library card. Any pin code data is retained securely by the Trust IT provider using encrypted data.

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

1. Legal framework

1.1 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'

1.2 This policy operates in conjunction with the following Trust policies:

- Data Protection Policy
- Trust Data Retention Policy

2. Definitions

2.1 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.

2.2 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.

2.3 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 staff and learners' biometric data, e.g. taking measurements from a fingerprint via a fingerprint scanner.
- Storing staff and learners' biometric information on a database.
- Using staff and 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.

2.4. 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.

3. Roles and responsibilities

3.1 The Trust Board is responsible for:
Reviewing this policy on an annual basis.

3.2 The Central Team and Principals at each school are responsible for:
Ensuring the provisions in this policy are implemented consistently.

3.3 The Data Protection Officer (DPO) and Trust GDPR Lead are responsible for:
Monitoring the Trust's compliance with data protection legislation in relation to the use of biometric data.
Advising on when it is necessary to undertake a data protection impact assessment (DPIA) in relation to the Trust/school's biometric system(s).
Being the first point of contact for the Information Commissioners Office (ICO) and for individuals whose data is processed by the Trust and its schools and connected third parties.

4. Data protection principles

4.1 The Trust processes all personal data, including biometric data, in accordance with the key principles set out in the GDPR.

4.2 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.

4.3 As the data controller, the Trust is responsible for being able to demonstrate its compliance with the provisions outlined in 4.2. The GDPR principles are detailed further in the Trust's Data Protection and Freedom of Information Policy (FOI) Policy. The Trust's DPO can be contacted at dpo@neneeducationtrust.org.uk

5. Notification and consent

Please note 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.

5.1 Where the Trust and its schools use staff and learners' biometric data as part of an automated biometric recognition system (e.g. using learners' fingerprints to receive school dinners instead of paying with cash or a PIN), the Trust and its schools will comply with the requirements of the Protection of Freedoms Act 2012.

5.2 Prior to processing a staff or learner's biometric data, the Trust or school will send the parents / carers a Trust Student Consent Form.

5.3 Written consent will be sought from at least one parent of the learner before the Trust or school collects or uses a learner's biometric data.

5.4 Notification sent to parents /carers will include information regarding the following:

- How the data will be used
- The right to refuse or withdraw their consent
- The Trust or school's duty to provide reasonable alternative arrangements for those learners whose information cannot be processed

5.5 The Trust/school 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

5.6 Parents and learners can object to participation in the Trust/school'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.

5.7 If a learner objects or refuses to participate, or to continue to participate, in activities that involve the processing of their biometric data, the school 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).

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

5.9 Where staff members or other adults use the Trust/school's biometric system(s), consent will be obtained from them before they use the system.

5.10 Staff and other adults can object to taking part in the Trust/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.

5.11 Alternative arrangements will be provided to any individual that does not consent to take part in the Trust/school's biometric system(s), in line with section 7 of this policy.

6. Alternative arrangements

6.1 Learners and staff have the right to not take part in the Trust/school's biometric system.

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

6.3 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).

7. Data retention

7.1 Biometric data will be managed and retained in line with the Trust's Data Retention Policy.

7.2 If an individual (or a learner's parent, where relevant) withdraws their consent for their biometric data to be processed, it will be erased from the Trust/school's system.

8. Breaches

8.1 There are appropriate and robust security measures in place to protect the biometric data held by the Trust/school.

8.2 Any breach to the Trust/school's biometric system(s) will be dealt with by the Trust's DPO and GDPR Lead.

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our Data Protection Officer:

Angela Corbyn on 07775 436141, email dpo@neneeducationtrust.org.uk, or leave a letter at our offices at the address below:

Nene Education Trust, Waterside House, Nene Business Centre, Station Road, Irthlingborough, Northamptonshire NN9 5QF

Nene Education Trust GDPR queries please contact:-

Victoria Brennan, Trust GDPR Lead 01933 400549
vbrennan@neneeducationtrust.org.uk