TMPF
PROTECTION OF BIOMETRIC INFORMATION OF CHILDREN IN SCHOOL
POLICY 2023

Ratified: March 2023

Review date: January 2024

Content Statement of intent

The Moorlands Primary Federation comprises seven schools: Bishop Rawle C. E. Primary School; Dilhorne Endowed C. E. Primary School; Great Wood Primary School; Hollinsclough C.E. Academy; Manifold C.E. Academy, St. Werburgh's C. E. Primary School; and The Valley Primary School.

TMPF Values:

Trust;
Mindful;
Peace;
Friendship.

Introduction
This policy relates to each school comprising The Moorlands Primary Federation (see above). From this point onwards, they will be referred to as the Trust or TMPF.

Statement of Intent
The Moorlands Primary Federation is committed to protecting the personal data of all its pupils and staff, this includes any biometric data we may collect and process.

We will 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 schools within TMPF follow when collecting and processing biometric data.

Biometric information and how it will be used
Biometric data is information about a person's individual physical, psychological, or behavioural characteristics that can be used to identify them, e.g. their fingerprints.
The information will be used as part of an automated biometric recognition system. This system will take measurements of the biometric information specified above and convert these measurements into a template to be stored on the system. An image of your child's biometric information is not stored. The template (i.e. the measurements taken from your child) may be used to permit your child to receive or pay for their school meal.

Providing your consent/objecting to the use of biometric data
Under the Protection of Freedoms Act 2012, schools are required to notify each parent of a child and obtain the written consent of at least one parent before being able to use any pupil's biometric information for an automated system. Where the name of only one parent is included on the admission register, consideration will be given to what reasonable steps should be undertaken to ascertain the details of the other parent.

Schools will not need to notify a particular parent or seek his or her consent if they are satisfied that:

a. The parent cannot be found, for example, his or her whereabouts or identity is not known;
b. The parent lacks the mental capacity to object or to consent;
c. The welfare of the child requires that a particular parent is not contacted, for example where a child has been separated from an abusive parent who is not to be informed of the child's whereabouts; or
d. Where it is otherwise not reasonably practical for a particular parent to be notified for his or her consent to be obtained.

Where neither of the parents of a child can be notified for one of the reasons set out above (which would mean consent cannot be obtained from either of them), section 27 of the Protection of Freedoms Act 2012 sets out who should, in such circumstances be notified and their written consent obtained.

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

1.2. This policy operates in conjunction with the following TMPF policies:

- TMPF Data Protection Policy
- TMPF Safeguarding 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 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.

2.3. **Processing biometric data:** Processing biometric data includes obtaining, recording or holding the data or carrying out any operation 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:

- Recording pupils' biometric data, e.g. taking measurements from a fingerprint via a fingerprint scanner.
- Storing learners' 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.

2.4. **Special category biometric data:** Personal data which UK GDPR says is more sensitive, and so needs more protection – where biometric data is

used for identification purposes, it is considered special category data. Data can only be processed when a legal basis has been identified under:

Article 6 UK GDPR - which sets out the lawful bases for processing data
. lawfulness, fairness and transparency.
. purpose limitation
. data minimisation
. accuracy
. storage limitation
. integrity and confidentiality
. accountability

Article 9 UK GDPR – which sets out the list of special categories of data and conditions for processing. Further conditions may also have to be satisfied under Schedule 1 of the Data Protection Act 2021.

3. Roles and responsibilities

3.1. The Moorlands Primary Federation is responsible for:

- Reviewing this policy on an annual basis.

3.2. The Executive Principals/CEO are responsible for:

- Ensuring the provisions in this policy are implemented consistently.

3.3. The Data Protection Officer (DPO) is responsible for:

- Monitoring TMPF'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 school's biometric system(s).
- Being the first point of contact for the ICO and for individuals whose data is processed by TMPF and connected third parties.

4. Data protection principles

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

4.2. TMPF 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, TMPF is responsible for being able to demonstrate its compliance with the provisions outlined in 4.2. The GDPR principles are detailed further in the TMPF Data Protection Policy. The Local Authority act as DPO for TMPF.

5. Data protection impact assessments (DPIAs)

5.1. Prior to processing biometric data or implementing a system that involves processing biometric data, a DPIA will be carried out.

5.2. The DPO and Executive Principals/CEO will oversee and monitor the process of carrying out the DPIA.

5.3. 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.

5.4. When assessing levels of risk, the likelihood and the severity of any impact on individuals will be considered.

5.5. If a high risk is identified that cannot be mitigated, the DPO will consult the ICO before the processing of the biometric data begins.

5.6. TMPF will adhere to any advice from the ICO.

6. 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 UK GDPR. Instead, the consent requirements for biometric information is imposed by the Protection of Freedoms Act 2012.

6.1. Where TMPF use pupils' biometric data as part of an automated biometric recognition system (e.g. using pupil' fingerprints to receive school dinners, the TMPF will comply with the requirements of the Protection of Freedoms Act 2012.

6.2. Prior to processing a pupil's biometric data, all schools within TMPF will notify parents, carers, legal guardians of its intention to process biometric information. Parents / carers/guardians will be provided with a Student Consent Form.

6.3. Written consent will be sought from at least one parent of the pupil before schools collects or uses a pupil's biometric data.

6.4. Notification sent to parents /carers/guardians 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.
- TMPF's duty to provide reasonable alternative arrangements for those pupils whose information cannot be processed.

6.5. The TMPF will not process the biometric data of a pupil under the age of 18 in the following circumstances:

- The pupil (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.

6.6 Parents and pupils can object to participation in the school's biometric system(s) or withdraw their consent at any time. Where this happens, any biometric data relating to the pupils that has already been captured will be deleted.

6.7. If a pupil objects or refuses to participate, or to continue to participate, in activities that involve the processing of their biometric data, school's will ensure that the pupil's biometric data is not taken or used as part of

a biometric recognition system, irrespective of any consent given by the pupil's parent(s).

6.8. Pupil's will be informed that they can object or refuse to allow their biometric data to be collected and used via the Consent Form.

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

6.10. Staff and other adults can object to taking part in 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.

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

7. Alternative arrangements

7.1. Pupils and staff have the right to not take part in TMPF's biometric system.

7.2. 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/receive school meals, the person will be able to use a 4 digit PIN instead.

7.3. 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 pupil's parents, where relevant).

8. Data retention

8.1. Biometric data will be managed and retained in line with TMPF's Records Management Policy.

8.2. 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 system.

9. Breaches

9.1 Any breach to the academy's biometric system(s) will be dealt with by the DPO to the TMPF.

Parents and pupils can object to participation in the biometric system(s) or withdraw their consent at any time. Where this happens, any biometric data relating to the pupil that has already been captured will be deleted.

CONSENT FORM FOR THE USE OF BIOMETRIC INFORMATION IN SCHOOL

Please complete this form if you consent to the school taking [and using information from your child's [*insert biometric – e.g. fingerprint*] by [*name of school*] as part of an automated biometric recognition system. This biometric information will be used by [*name of school*] for the purpose of [*describe purpose(s) for which this data will be used, e.g. administration of school canteen*].

In signing this form, you are authorising the school to use your child's biometric information for this purpose until he/she either leaves the school or ceases to use the system. If you wish to withdraw your consent at any time, this must be done so in writing and sent to the school at the following address:

[*insert address*]

Once your child ceases to use the biometric recognition system, his/her biometric information will be securely deleted by the school.

Having read guidance provided to me by [*name of school/college*], I give consent to information from the [*insert biometric – e.g. fingerprint*] of my child:

[insert *name of child*]

being taken and used by [*name of school*] for use as part of an automated biometric recognition system for [*describe purpose(s) for which this data will be used, e.g. administration of school canteen*].

I understand that I can withdraw this consent at any time in writing.

Name of Parent: ……..

Signature: ……

Date: ……

Please return this form to: [*insert suitable delivery point and name of school*].