DATA AND INFORMATION GOVERNANCE:

Protection of Biometric Information Policy

This policy has been adopted by the Board of Directors of Pathfinder Multi Academy Trust and is applicable across all schools that make up the Trust. In line with the MAT's Scheme of Delegation, this Policy must be duly applied by each Local Governing Committee and the Headteacher of each school that is part of Pathfinder Multi Academy Trust.

Where there are specific details or any discretions in the policy that apply to an individual school or Local Governing Committee this has been made clear within the wording of the policy.

This policy will be reviewed formally by the MAT Board of Directors in line with the agreed timetable for policy review or sooner as events or legislation changes require.

Date Adopted: **March 2021**

Date for Review: **March 2022**

Contents

1 Introduction

The Protection of Biometric Information Policy outlines the procedure Pathfinder Multi Academy Trust (PMAT) follows when collecting and processing special category biometric data.

The Policy governs Pathfinder Multi Academy Trusts collection and processing of biometric data. The nature of this processing, including what information is processed and for what purpose, is outlined in the Pathfinder Multi Academy Trusts school's privacy notice.

Pathfinder Multi Academy Trust will comply with the additional requirements of sections 26 to 28 of the Protections of Freedoms Act 2012, this includes provisions which relate to the use of biometric data in schools and colleges who use an automated biometric recognition system. These provisions are in addition to the requirements of GDPR.

This policy complements the Trust's existing records of processing required under Article 30 of the General Data Protection Regulation (GDPR) 2018, which is fulfilled through the Trust's Information Asset Register. It should also be read in conjunction with the other policies and privacy notices in the Trust's Information Governance policy and privacy notice framework.

2 Scope

All policies in PMAT's Data and Information Governance policy framework apply to all PMAT employees, any authorised agents working on behalf of PMAT, including temporary or agency employees, and third party contractors. Individuals who are found to knowingly or recklessly infringe these policies may face disciplinary action.

The policies apply to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper,
- Information or data stored electronically, including scanned images,
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer,
- Information or data stored on or transferred to removeable media such as tape, CD, DVD, USB storage device or memory card,
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops,
- Speech, voice recordings and verbal communications, including voicemail,
- Published web content, for example intranet and internet,
- Photographs and other digital images.

3 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. For example, where a fingerprint is used to identify an individual and allow them access to an account.

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. Biometric Data is defined in the GDPR 2018 and the Data Protection Act 2018 as a special category of personal data, and it therefore requires additional measures to be put in place in order to process it, as detailed below.

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 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.

Any processing of Biometric data will only be carried out where there is a lawful purpose for the processing, as defined under Article 6 and Article 9 (Schedule 1) of the GDPR 2018. The purposes will be outlined in the PMAT school's privacy notices which will be made available to the relevant individuals.

4 Roles and responsibilities

The Trust board is responsible for:

- Reviewing this policy on an annual basis.

The headteacher is responsible for:

- Ensuring the provisions in this policy are implemented consistently within schools.

The data protection officer (DPO) is responsible for:

- Monitoring the school'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 the Trust and connected third parties.

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.

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 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 Trust with a written response (within eight weeks or 14 weeks in complex cases) advising whether the risks are acceptable, or whether the Trust needs to take further action. In some cases, the ICO may advise the Trust to not carry out the processing.

The Trust will adhere to any advice from the ICO.

7 What Counts as Valid 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.

Where the school uses pupils' biometric data as part of an automated biometric recognition system (e.g. using pupils' fingerprints to receive school dinners instead of paying with cash), the school will comply with the requirements of the Protection of Freedoms Act 2012.

All consent must be freely-given, specific, informed and unambiguous, and will be obtained through a clear affirmative action. The PMAT school will collect consent as noted below:

Prior to any biometric recognition system being put in place or processing a pupil's biometric data, the school will send the pupil's parents a Parental Notification and Consent Form for the use of Biometric Data.

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

The name and contact details of the pupil's parents will be taken from the school's admission register.

Where the name of only one parent is included on the admissions register, the headteacher 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, e.g. their whereabouts or identity is not known.
- The parent lacks the mental capacity to object or consent.
- The welfare of the pupil requires that a particular parent is not contacted, e.g. where a pupil has been separated from an abusive parent who must not be informed of the pupil's whereabouts.
- It is otherwise not reasonably practicable for a particular parent to be notified or for their consent to be obtained.

Where neither parent of a pupil can be notified for any of the reasons set out above, consent will be sought from the following individuals or agencies as appropriate:

- If a pupil is being 'looked after' by the LA or is accommodated or maintained by a voluntary organisation, the LA or voluntary organisation will be notified and their written consent obtained.
- If the above does not apply, then notification will be sent to all those caring for the pupil and written consent will be obtained from at least one carer before the pupil's biometric data can be 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 school's duty to provide reasonable alternative arrangements for those pupils whose information cannot be processed

A school 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

A school will not process the biometric data of a pupil aged 12 to 18 years old 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

Parents and pupils can object to participation in the school's biometric system(s) or withdraw their consent at any time. Consent can be withdrawn at any time by the parent/carer or the individual, by contacting the school. Where this happens, any biometric data relating to the pupil that has already been captured will be deleted.

If a pupil 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 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).

Pupils will be informed that they can object or refuse to allow their biometric data to be collected and used via a letter.

Where staff members or other adults use the school'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 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.

The consent will be valid until it is withdrawn or until the Biometric data reaches the PMAT retention period, as outlined in the PMAT retention schedule and Information Asset Register/ when the student leaves the school, at which point the Biometric data and record of consent will be securely destroyed.

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.

8 Alternative arrangements

Parents, pupils, staff members and other relevant adults have the right to not take part in the school's biometric system(s).

Where an individual objects to taking part in the school'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 pupil's fingerprints to pay for school meals, the pupil will be able to use another method for the transaction.

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).

9 Data retention

Biometric data will be managed and retained in line with the Trust's Records Management 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 school's system.

10 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 Trust's Information Security Policy.

Any breach to the school's biometric system(s) will be dealt with in accordance with the Information Security Policy.