Protection of Biometric Information Policy v1.0

Important: This document can only be considered valid when viewed on the Trust website. If this document has been printed or saved to another location, you must check that the version number on your copy matches that of the document online. **Name and Title of Author:**	Francesca Roper, Director of Trust Development and Compliance
Name of Responsible Committee/Individual:	Audit and Risk Committee
Implementation Date:	Spring 2023
Review Date:	Spring 2025
Related Documents:	Data Protection Policy TEAL Data Breach Guidance Data Protection Impact Assessment (DPIA) Subject Access Request (SAR) Guidance TEAL Retention Guidelines

Protection of Biometric Information

Contents:

1 Policy statement

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 ▪ UK General Data Protection Regulation (UK GDPR)

▪ DfE (2018) 'Protection of biometric information of children in schools and colleges'

1.2 This policy operates in conjunction with the following Trust policy and procedures:

▪ Data Protection Policy ▪ Data Breach Guidance ▪ Data Protection Impact Assessment (DPIA) ▪ Subject Access Request (SAR) Guidance ▪ TEAL Retention Guidelines

2 About this policy

2.1 This policy and any other documents referred to in it set out the basis on which we will process any biometric information we collect from data subjects, or that is provided to us by data subjects or other sources.

2.2 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.3 This policy sets out rules on protecting biometric information and the legal conditions that must be satisfied when we process biometric information.

3 Definition of biometrics information terms

3.1 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.

3.2 Biometric information: 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.

3.3 Consent: GDPR requires that consent must be freely given, that the trust must keep a record to demonstrate consent; be able to display prominence and clarity of consent requests; and advise the right to withdraw consent easily and at any time.

3.4 Data controller: Under data protection law, the Trust is the data controller for all biometric information held by the schools.

3.5 Processing biometric information: Processing biometric information 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 information, e.g. taking measurements from a fingerprint via a fingerprint scanner.
- Storing pupils' biometric information on a database.
- Using pupils' biometric information as part of an electronic process, e.g. by comparing it with biometric information stored on a database to identify or recognise pupils.

3.6 Special category data: Personal data which the GDPR says is more sensitive, and so needs more protection – where biometric information is used for identification purposes, it is considered special category data.

4 Roles and responsibilities

4.1 The Audit and Risk Committee are responsible for approving this policy.

4.2 The Director of Trust Development and Compliance is responsible for ensuring the provisions in this policy are implemented consistently.

4.3 The Trust's Data Protection Officer (DPO) is responsible for;

- Monitoring the school's compliance with data protection legislation in relation to the use of biometric information.
- Advising on when it is necessary to undertake or amend a data protection impact assessment (DPIA) in relation to the academy's biometric system(s).
- Being the first point of contact for the Information Commissioners Office (ICO).

5 Data protection principles

5.1 The trust processes all personal data, including biometric information, in accordance with the key principles set out in the GDPR.

5.2 The trust must ensure biometric information 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.

6 Data protection impact assessments (DPIAs)

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

6.2 The DPO controls the Data Protection Impact Assessment (DPIA) procedure for the Trust and must be contacted prior to beginning a DPIA.

6.3 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.

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

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

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

6.7 The Trust will adhere to any advice from the ICO.

7 Consent

7.1 Prior to any biometric recognition system being put in place or processing of biometric information, the trust via the schools must request written consent for the use of biometric information.

7.2 Consent must be freely given. Schools must request written consent advising an explicit yes or no answer to consenting to the processing of biometric information.

7.3 Consent must not be gained through an opt-out option.

7.4 If there is no reply to the consent request, the school must determine this as consent is not provided.

7.5 The school must keep a record of consent as part of the pupil/staff file.

7.6 Request for consent from individuals must advise the following:

- Details about the type of biometric information to be taken
- Details of the system(s) that will be used to hold and process the biometric information
- How the biometric information will be used
- The right to refuse or withdraw their consent
- The school's duty to provide reasonable alternative arrangements for those pupils whose information cannot be processed

7.7 Consent can be withdrawn at any time, see 8.6 for withdrawal of pupil biometric information, and 9.2 for staff withdrawal.

7.8 Alternative arrangements must be provided to any individual that does not consent to take part in the school's biometric system(s), in line with section 10 of this policy.

8 Pupil consent

8.1 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.

8.2 The written consent of at least one parent must be obtained before the data is taken from the pupil and used. This applies to all pupils under the age of 18. In no circumstances can a pupil's biometric information be processed without written consent from parents.

8.3 Schools must ensure that each parent of a child is notified of the school's intention to use a pupil's biometric information as part of an automated biometric recognition system.

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

- If a pupil is being 'looked after' by the Local Authority (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 information can be processed.

8.5 The school will not process the biometric information 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 information
- No parent or carer has consented in writing to the processing.
- A parent or carer of the pupil has objected in writing to such processing, even if another parent has given written consent.

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

8.7 If a pupil objects or refuses to participate, or to continue to participate, in activities that involve the processing of their biometric information, the school will ensure that the pupil's biometric information is not taken or used as part of a biometric recognition system, irrespective of any consent given by the pupil's parent(s).

8.8 Consent is considered valid for the duration of a pupils for the duration that the pupil is on roll at the school unless consent is withdrawn by the pupil or parent.

9 Staff consent

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

9.2 Staff and other adults can object to taking part in the school's biometric system(s) and can withdraw their consent at any time. This must be in writing. Where this happens, any biometric information relating to the individual that has already been captured must be deleted.

9.3 For staff, consent is considered valid for the duration of employment, unless consent is withdrawn.

10 Alternative arrangements

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

10.2 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 a pre-programmed card, unique number or other suitable means determined by the school.

10.3 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).

11 Data retention

11.1 Biometric information will be managed and retained in line with the Trust's retention schedule.

11.2 If an individual (or a pupil's parent, where relevant) withdraws their consent for their/their child's biometric information to be processed, it must be erased from the school's system(s) without undue delay.

12 Data breaches

.

12.1 The Director of IT is responsible for ensuring there are appropriate and robust security measures in place to protect the biometric information held by the school.

12.2 Any suspected data breach must be immediately reported to the Headteacher and the Trust's Data Protection Officer (DPO).

12.3 Any suspected data breach to the school's biometric system(s) will be dealt with in accordance with the Trust's Data Protection Policy and be reviewed using the Trust's Data Breach Procedure.

13 Subject access requests (SAR)

13.1 Any subject access requests (SAR) for biometric information will be dealt with in accordance with the Trust's Data Protection Policy and be reviewed using the Trust's Subject Access Request (SAR) Guidance.

14 Monitoring and review

14.1 The Audit and Risk Committee are responsible for reviewing this policy.

14.2 Any changes made to this policy will be communicated to the schools within the Trust advising any necessary actions.