Biometrics policy

Approved by:	Deputy Chief Operating Officer **Date:** 27 July 2021
Last reviewed on:	14 October 2021 (by the Board of Trustees
Next review due by:	September 2022

1 What is biometric data?

1.1 Biometric data means personal information about an individual's physical or behavioural characteristics that can be used to identify that person; this can include their fingerprints, facial shape, retina and iris patterns, and hand measurements.

1.2 All biometric data is considered to be special category data under the UK General Data Protection Regulation (UK GDPR). This means the data is more sensitive and requires more protection and this type of data could create more significant risks to a person's fundamental rights and freedoms.

1.3 This policy complies with The Protection of Freedoms Act 2012 (sections 26 to 28), the Data Protection Act 2018 and the UK GDPR.

1.3 The trust has carried out a data protection impact assessment with a view to evaluating whether use of biometric data is a necessary and proportionate means of achieving the legitimate objectives set out below.

1.4 The result of the data protection impact assessment has informed the trust's use of biometrics and the contents of this policy.

2 What is an automated biometric recognition system?

2.1 An automated biometric recognition 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.

3 The legal requirements under UK GDPR.

3.1 'Processing' of biometric information includes obtaining, recording or holding the data or carrying out any operation or set of operations on the data including (but not limited to) disclosing it, deleting it, organising it or altering it.

3.2 As biometric data is special category data in order to lawfully process this data, the trust must have a legal basis for processing personal data and a separate condition for processing special category data. When processing biometric data, the trust relies on explicit consent (which satisfies the fair processing conditions for personal data and special category data). Consent is obtained using the consent form(s) in the attached appendicies.

3.3 The trust's academies process biometric data as an aim to make significant improvements to the provision and payment of school meals. This is to ensure

efficiency; to eliminate the need for cash being used and to streamline the delivery of school meals.

4 Consent and withdrawal of consent.

4.1 The trust will not process biometric information without the relevant consent.

4.2 Consent for pupils

4.2.1 When obtaining consent for pupils, parents will be notified that the individual school intends to use and process their child's biometric information. The school only require written consent from one parent (in accordance with the Protection of Freedoms Act 2012), provided no parent objects to the processing.

4.2.2 If a parent objects to the processing, then the school will not be permitted to use that child's biometric data and alternatives will be provided.

4.2.3 The child may also object to the processing of their biometric data. If a child objects, the school will not process or continue to process their biometric data, irrespective of whether consent has been provided by the parent(s).

4.2.4 Where there is an objection, the school will provide reasonable alternatives which will allow the child to access the same facilities that they would have had access to had their biometrics been used.

4.2.5 Students and parents can also object at a later stage to the use of their child's/their biometric data. Should a parent wish to withdraw their consent, they can do so by writing to the school using the relevant email address requesting that the school no longer uses their child's biometric data.

4.2.6 Students who wish for the school to stop using their biometric data do not have to put this in writing but should let their pastoral lead know.

4.2.7 The consent will last for the time period that your child attends the school (unless it is withdrawn).

4.3 Consent for staff

4.3.1 The school will seek consent of staff before processing their biometric data.

4.3.2 If the staff member objects, the school will not process or continue to process the biometric data and will provide reasonable alternatives. Staff who wish for the school to stop using their biometric data should do so by writing to the Principal.

4.3.3 The consent will last for the time period that the staff member remains employed by the trust (unless it is withdrawn).

5 Retention of Biometric Data

5.1 Biometric data will be stored by the school for as long as consent is provided (and not withdrawn).

5.2 Once a student or staff member leaves, the biometric data will be deleted from the school's system no later than 72 hours.

5.3 At the point that consent is withdrawn, the school will take steps to delete their biometric data from the system and no later than 72 hours.

6 Storage of Biometric Data

6.1 Biometric data will be kept securely and systems will be put in place to prevent any unauthorised or unlawful access/ use.

6.2 The biometric data is only used for the purposes for which it was obtained and such data will not be unlawfully disclosed to third parties.

Appendix 1: Biometric consent form (parent/carer)

Please sign below if you consent to the school taking and using information from your son/daughter's fingerprint or facial recognition as part of an automated biometric recognition system. This biometric information will be used by the school for the purpose of administration of school meals.

In signing this form, you are authorising the school to use your son/daughter'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 Principal. Once your son/daughter ceases to use the biometric recognition system, his/her biometric information will be securely deleted by the school no later than 72 hours.

Parent consent:

Having read the above guidance information, I give consent to information from the fingerprint or facial recognition of my son/daughter being taken and used by the school for use as part of an automated biometric recognition system.

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

Parent/ carer name:	
Signature:	
Date:	
Name of student:	

Please send a copy of this consent form to [each school to amend with individual contact details]

Appendix 2: Biometric consent form (staff)

Please sign below if you consent to the school taking and using your fingerprint or facial recognition information as part of an automated biometric recognition system. This biometric information will be used by the school for the purpose of administration and supply of food and meals through the school's catering provider.

In signing this form, you are authorising the school to use your biometric information for this purpose until you either leave the school or cease 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 Principal.

Having read the above guidance information, I give consent to information from my fingerprint or facial recognition being taken and used by the school for use as part of an automated biometric recognition system.

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

Staff name:	
Signature:	
Date:	

Please send a copy of this consent form to [each school to amend with individual contact details]