



Biometrics Policy

December 2025

Reviewed by Executive Team:	November 2025
Endorsed by [committee]:	N/A
Approved by Board:	9 December 2025
Next review	Autumn 2027

1. Introduction

- 1.1 The UK General Data Protection Regulation (UK GDPR) ensures a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.
- 1.2 Horsham Learning Alliance (the Trust) and its College/schools will protect and maintain a balance between data protection rights in accordance with the UK GDPR in respect of how we handle the biometric data. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

The Trust's registration number is ZB964470. This registration is renewed annually and up dated as and when necessary.

2. Biometric data

- 2.1 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.
- 2.2 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 additional protection as this type of data could create more significant risks to a person's fundamental rights and freedoms.

This policy complies with The Protection of Freedoms Act 2012, the Data Protection Act 2018 and the UK GDPR.

3. Automated Biometric Recognition System

- 3.1 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.

4. The Legal Requirements under UK GDPR

- 4.1 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.
- 4.2 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 College/schools rely on explicit consent (which satisfies the fair processing

conditions for personal data and special category data). Consent is obtained using our admission form when students start at the College/schools.

- 4.3 The aim of processing biometric data is to make significant improvements to canteen and lunch facilities. This is to ensure efficiency and eliminate the need for swipe cards and cash being used and to make sure the student is only purchasing food for themselves.

5. Consent and Withdrawal of Consent

- 5.1 The College/schools will not process biometric information without the relevant consent. For a student below the age of 13, consent will need to be sought from a parent/carer. When obtaining consent for students, both parents/carers will be notified how the College/schools will use and process their child's biometric information. The College/schools only requires written consent from one parent/carer (in accordance with the Protection of Freedoms Act 2012), provided no parent/carer objects to the processing. Students aged 13 or over may provide their own consent for processing biometric data.
 - 5.2 For a student below the age of 13, if a parent/carer objects to the processing, then the College/schools will not be permitted to use that child's biometric data and alternatives will be provided.
 - 5.3 Even if a parent/carer has provided consent for their child below the age of 13, the child may also object to the processing of their biometric data. If a child objects, the College/schools will not process or continue to process their biometric data, irrespective of whether consent has been provided by the parent(s)/carer(s).
 - 5.4 Where there is an objection, the College/schools will provide reasonable alternatives which will allow the child to access the same facilities that they would have had access to if their biometrics been used.
 - 5.5 Students and parents/carers can also object at a later stage to the use of their own/their child's biometric data. Should a parent/carer wish to withdraw their consent, they can do so by writing to the College/school office requesting that the College/schools no longer use their child's biometric data.
 - 5.6 The consent will last for the time period that your child attends a College/schools within the Trust (unless it is withdrawn) and this will be transferred within the College/schools in the Trust, providing this is for the purposes of standard transition from one education phase to the next (i.e. primary to secondary, secondary to post-16).
- ## 6. Retention of Biometric Data
- 6.1 Biometric data will be stored by the College/schools for as long as consent is provided (and not withdrawn). Once a student leaves or withdraws consent, the biometric data will be deleted from the Trust's system no later than 1 month after they have left.

7. Storage of Biometric Data

- 7.1 At the point that consent is withdrawn, the College/schools will take steps to delete their biometric data from the system and no later than 1 month after they have left.
- 7.2 Biometric data will be kept securely and systems will be put in place to prevent any unauthorised or unlawful access/use. Biometric data (fingerprints) are stored as a series of data points, converted from images by a mathematical algorithm. These data points cannot be used to reconstruct a useable fingerprint even with the algorithm available. The level of detail stored in these data points is well below the level of detail needed for forensic identification of someone and would be completely inadmissible, both in terms of quality and legality, in court. The data points are encrypted before being stored.
- 7.3 The AES 256 encryption standard is used for storing top secret designated data by the American military and the NSA. Both AES and RSA are well used and commonly understood encryption standards that cannot be broken by brute force in a reasonable time.
- 7.4 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.

8. Related Documentation

This policy links to the following policies and procedures:

- Data Protection Policies
- Freedom of Information Policy
- Data Retention