OVERTON GRANGE SCHOOL
POLICY (Statutory)

BIOMETRIC DATA POLICY

Govs Comm. RESOURCES COMMITTEE

Reason for the Policy

The reason for this policy is to enable the use of software that uses facial recognition to process cashless catering at Overton Grange School. This will enable students and staff to use contactless purchasing of food and beverages, as well as giving them greater security over their user identity.

Principles

Under the GDPR, personally identifiable data is defined as 'special category' personal data, which means that explicit consent is required from an individual to use the biometric data.

1. What is biometric data?

Biometric data means personal information resulting from specific technical processing relating to an individual's physical, psychological or behavioural characteristics which allow or confirm the unique identification of that person, such as facial images, voice recognition or fingerprints.

The Data Protection Action 2018, UK GDPR, and the protection of Freedoms Act 2012 set out how students' data (including biometric data) should be processed.

Biometric data is special category data and must be processed lawfully, fairly and in a transparent way. More information can be found on this in the Data protection policy.

2. What is an automated biometric recognition system?

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). Biometric systems usually store measurements taken form a person's physical/behavioural characteristics and not images of the characteristics themselves.

Biometric recognition systems can use many kinds of physical or behavioural characteristics such as those listed in 1) above.

3. What is Facial recognition?

Facial recognition is the process by which a person can be identified or otherwise recognised from a digital facial image. Cameras are used to capture these images and facial recognition technology software produces a biometric template. Often, the system will then estimate the degree of similarity between two facial templates to identify a match (e.g. to verify someone's identity), or to place a template in a particular category (e.g. age group). This type of technology can be used in a variety of contexts from unlocking our mobile phones, to setting up a bank account online, or passing through passport control.

Facial recognition is used by students when paying for school lunches as it is both necessary and proportionate within the school environment.

We do not use live facial recognition in school.

4. What does processing data mean?

'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. An automated biometric recognition system processes data when:

a) Recording students' biometric data, for example, mapping an individual's facial features (such as the length and width of the nose, the distance between the eyes and the shape of the cheekbones);
b) Storing students' biometric information on a database system; or
c) Using that data as part of an electronic process, for example, by comparing it with biometric information stored on a database in order to identify or recognise students.

What is the policy going to do?

Based on current legislation:

- Schools and colleges that use student biometric data must treat the data collected with appropriate care and must comply with the data protection principles as set out in the Data Protection Act 2018 and with UK GDPR.
- Where the data is to be used as part of an automated biometric recognition system, schools and colleges must also comply with the additional requirements in sections 26 to 28 of the Protection of Freedoms Act 2012.
- Under Article 35 of the UK GDPR, the data controller must identify additional risks associated with using automated biometric technology by conducting a DPIA ensuring decisions are documented.
- Schools and colleges must ensure that each parent/carer of a child is notified of the school's intention to use the child's biometric data as part of an automated biometric recognition system.
- The written consent of at least one parent must be obtained before the data is taken from the child and used (i.e. 'processed' – see 3 above, and no parent/carer has withdrawn his/her consent, or otherwise objected, to the information being processed. This applies to all pupils in schools and colleges under the age of 18. **In no circumstances can a child's biometric data be processed without written consent.**

- Schools and colleges must not process the biometric data of a pupil (under 18 years of age) where:
    a) The child (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data. A student's objection or refusal overrides any parental consent to the processing;
    b) No parent has consented in writing to the processing; or
    c) A parent has objected in writing to such processing, even if another parent has given written consent.
- Schools and colleges must provide reasonable alternative means of accessing services for those pupils who will not be using an automated biometric recognition system.

How is the policy going to be put into practice?

The school will:

- Collect biometric consent when a student first joins the school, via the school admission form
- Record consent on the student file on SIMS
- Ensure that students understand that they can object or refuse to allow their biometric data to be taken/used
- Provide the opportunity for students and staff to register their biometric data (facial recognition) for the purpose of paying for food in the canteen
- Provide students and staff with a 6-digit PIN code or other suitable alternative where biometric consent is withheld
- Ensure that biometric data is only used for the purposes of purchasing food and that the data is not unlawfully disclosed to third parties
- Once a student or member of staff stops using the biometric system, their biometric information will be securely deleted by the school

Criteria for success

- Parental consent obtained and recorded on SIMS
- Students and staff successfully registered and making use of the automated biometric system in the canteen
- Students provided with a 6-digit PIN code as an alternative to facial recognition if consent is not provided or is withdrawn.
- Biometric data securely deleted by the school once a student or member of staff stops using the biometric system

Monitoring and evaluation

- This policy will be regularly reviewed by SLT and Governors

Links with other policies

- Data Protection
- Privacy notices

Appendix:

1) Frequently Asked Questions

Associated Resources:

Protection of Freedoms Act 2012: CHAPTER 2 Protection of biometric information of children in schools etc.
https://www.legislation.gov.uk/ukpga/2012/9/contents/enacted

Data Protection Act 2018
https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

DfE Protection of biometric information of children in schools and colleges
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1092507/Biometrics_Guidance_July_2022.pdf

ICO guide to the General Data Protection Regulation:
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

British Standards Institute guide to biometrics:
http://shop.bsigroup.com/en/Browse-by-Subject/Biometrics/?t=r

Approved by:	Resources Committee Full Governing Body	**Date:** 6th March 2024 **Date:** 21st March 2024
Last reviewed on:	March 2024	
Next review due by:	March 2025	