

WICKERSLEY

SCHOOL & SPORTS COLLEGE

POLICIES

BIOMETRICS DATA POLICY



Biometric Data Policy

Key Points

- ❖ Schools and colleges that use pupils' **biometric data** must treat the data collected with appropriate care and must comply with the data protection principles as set out in the General Data Protection Regulations (GDPR) 2018.
- ❖ 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**.
- ❖ The Academy must ensure that each parent of a child is notified of the Academy'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 ie, '**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. If a parent wishes to withdraw consent please email or contact Wickersley school.
- ❖ 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;
 - 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.

1. What is biometric data?

- 1.1 *Biometric data* means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allows or confirms the unique identification of that natural person, such as facial images or dactyloscopic data.
 - 1.2 The Information Commissioner considers all biometric information to be sensitive personal data as defined by the **GDPR 2018**; this means that it must be obtained, used and stored in accordance with that Regulation.
 - 1.3 The Protection of Freedoms Act 2012 includes provisions which relate to the use of biometric data in schools and colleges when used as part of an automated biometric recognition system. These provisions are in addition to the requirements of the GDPR 2018.
- 2.2 Biometric recognition systems can use many kinds of physical or behavioural characteristics such as those listed in 1.1 above.

3. 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 pupils' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner;
- b) Storing pupils' 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 pupils.

Associated Resources

- [ICO guide to data protection](#)
- [ICO guidance on data protection for education establishments](#)
- [British Standards Institute guide to biometrics](#)