Royal Alexandra & Albert School

Biometric Data Policy

Policy applies to	All school pupils
Committee responsible	Pupil Matters
Governing Body approval required	Yes
Accountable Executive	Senior Assistant Head
Status & Review Cycle	Statutory / Annual
Last approval	PM 8 November 2022 / GB 21 March 23 meeting
Next approval	Spring 2024

Table of Contents

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 and Data Protection Act 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 School must ensure that each parent 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'**. 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. Pupils who are 18 years old will be asked directly for their 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;

    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. 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.

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.

4. Biometric Data at The School

Parental consent is provided via a form to parents. The consent is then logged on SIMs and can be withdrawn at any time by phone call or email. Any Pupil that is 18 years of age will be asked directly for their consent and not parents. Fingerprint data is held securely and is retained for the duration of the child's time at the school. Finger print data is used exclusively for our boarding signing in and out system 'Reach'.

Further Information

This document uses the term "The School" as set out in the Joint Controller and Information Sharing Framework Agreement – Between The Royal Alexandra and Albert School And The Royal Alexandra and Albert School Charitable Foundation