Biometric Information Policy

Policy Date: June 2026
Author: Operations Manager
Authorised by: Governing Body
Review Frequency: 2 years
Review Date: June 2028

Introduction

1 This policy sets out how Ringwood School process **biometric data**.

2 The Academy may use biometric information (for example, data sets taken from fingerprints or facial scans as part of an automated recognition system for the purposes of paying for school meals). Information from the individual is automatically compared with biometric information stored in a system to see if there is a match, in order to recognise or identify the individual.

3 All definitions highlighted in **bold** in this policy are defined fully in our Data Protection Policy.

4 We will comply with the additional requirements of sections 26 to 28 of the Protections of Freedoms Act 2012. This includes provisions which relate to the use of **biometric data** in schools and colleges who use an **automated biometric recognition system**. These provisions are in addition to the requirements of **data protection legislation**.

5 Additionally, we follow and comply with the non-statutory guidance provided by the Department for Education in the document 'Protection of biometric data of children in schools and colleges'.

Definitions of biometric data and processing

6 **Biometric data** is personal information about an individual's physical or behavioural characteristics that can be used to identify that person. Biometric data includes, but is not limited to fingerprints, facial shape, retina and iris patterns, and hand measurements, or references or data points taken from these features. Biometric data is defined in **data protection legislation** as a **special category of personal data**, and it therefore requires additional measures to be put in place to process it.

7 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. To be recognised, an individual must have been previously been subject to "enrolment". This is the process where samples of biometric data, such as fingerprints or a facial scan, are captured from an individual and stored to allow comparison in the future.

8 **'Processing' of biometric data** includes obtaining, recording, storing, disclosing, analysing, using, deleting, organising or modifying it. An automated biometric recognition system processes data when:

8.1 Biometric data is recorded, for example, capturing a fingerprint via a fingerprint scanner or a facial scan from a digital photograph.

8.2 Storing biometric information on a database or as part of a purchased system.

8.3 Using the recorded biometric data as part of an electronic process, to identify or recognise individuals.

Consent

9 For the purposes of **processing biometric data** of children in a school setting, the lawful basis is 'explicit consent' under **data protection legislation**. Additionally, there is a requirement for consent for processing children's biometric information imposed by section 26 of the Protection of Freedoms Act 2012.

10 The written consent of at least one parent must be obtained before the **biometric data** is taken from the child and used. This applies to all pupils in schools and colleges under the age of 18. In no circumstances will a child's **biometric data** be **processed** without written consent.

11 Where the Academy only holds contact information for only one parent, staff will consider whether any reasonable steps can or should be taken to ascertain the details of the other parent. The school does not need to notify a particular parent or seek their consent if it is satisfied that:

11.1 The parent cannot be found, after reasonable steps have been taken; or

11.2 The parent lacks the mental capacity to object or consent; or

11.3 Welfare or safeguarding concerns require that a particular parent is not to be contacted; or

11.4 It is not practicable for a particular parent to be contacted.

12 In addition, even if a parent consents, the child may object to the **processing** of **their biometric data** or refuse to cooperate with the **biometric data** collection or use. The child's objection/refusal takes precedent over the parents' consent.

13 For the purposes of processing **biometric data** of adults, the lawful basis is 'explicit consent' under **data protection legislation**.

14 The Academy has measures in place to ensure both children and adults can still access all services that the **biometric data processing** is designed to allow access to where consent is either withheld or withdrawn. The alternative arrangements will not put an individual at any disadvantage, create access difficulties or result in additional burdens.

Security and retention

15 Where a new system involving **biometric data**, or a new form of **processing biometric data** is introduced, or systems or processes are changed the Academy will ensure that a **DPIA** is completed as set out in our Data Protection Impact Assessment Procedure.

16 We will ensure that we store any **biometric data** securely to prevent any unauthorised or unlawful use, and only use it for the purposes it was obtained.

17 **Biometric data** will be securely destroyed in line with our Data Retention Policy, or when consent is withdrawn.

Review

18. This policy will be reviewed every 2 years by the Data Protection Officer.