Biometric Data Policy

Policy Number:	YH050
Version:	V01
Date of issue:	June 2025
Date of Next Review:	June 2026
Policy Author:	School Pro / Doug Grieb – Head of Operations
Ratified by:	Liam Gaster – Head Teacher

This policy is one of a series of school policies that, taken together, are designed to form a comprehensive statement of the school's aspiration to provide an outstanding education for each of its students and of the mechanisms and procedures in place to achieve this. Accordingly, this policy should be read alongside these policies. In particular it should be read in conjunction with the policies covering equality and diversity, Health and Safety, safeguarding and child protection.

All of these policies have been written, not simply to meet statutory and other requirements, but to enable and evidence the work that the whole school is undertaking to ensure the implementation of its core values.

While this current policy document may be referred to elsewhere in Yarrow Heights School documentation, including particulars of employment, it is non-contractual.

In the school's policies, unless the specific context requires otherwise, the word "parent" is used in terms of Section 576 of the Education Act 1996, which states that a 'parent', in relation to a child or young person, includes any person who is not a biological parent but who has parental responsibility, or who has care of the child. Department for Education guidance Understanding and dealing with issues relating to parental responsibility updated August 2023 considers a 'parent' to include:

- all biological parents, whether they are married or not
- any person who, although not a biological parent, has parental responsibility for a child or young person - this could be an adoptive parent, a step-parent, guardian or other relative
- any person who, although not a biological parent and does not have parental responsibility, has care of a child or young person

A person typically has care of a child or young person if they are the person with whom the child lives, either full or part-time and who looks after the child, irrespective of what their biological or legal relationship is with the child.

The school contracts the services of third-party organisations to ensure regulatory compliance and implement best practices for:

- HR and Employment Law
- Health & Safety Guidance
- DBS Check processing
- Mandatory Safeguarding, Health & Safety, and other relevant training
- Data protection and GDPR guidance
- Specialist insurance cover

Where this policy refers to 'employees', the term refers to any individual that is classified as an employee or a worker, working with and on behalf of the school (including volunteers and contractors).

The school is committed to safeguarding and promoting the welfare of children and young people and expects all staff, volunteers, pupils and visitors to share this commitment.

All outcomes generated by this document must take account of and seek to contribute to safeguarding and promoting the welfare of children and young people at Yarrow Heights School.

The policy documents of Yarrow Heights School are revised and published periodically in good faith. They are inevitably subject to revision. On occasions a significant revision, although promulgated in school separately, may have to take effect between the re-publication of a set of policy documents. Care should therefore be taken to ensure, by consultation with the Senior Leadership Team, that the details of any policy document are still effectively current at a particular moment.

Document Version Control Log

Version	Date	Description of changes and person/organisation responsible
2.0	20/01/2021	Text updated to reflect end of Brexit transition and updates references from the General Data Protection Regulation (GDPR) to the UK General Data Protection Regulation (UK GDPR). (SchoolPro TLC)

Contents

1. Introduction

What is Biometric Data?

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.

Schools and academies 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 UK General Data Protection Regulation.

The Information Commissioner considers all biometric information to be personal data as defined by the UK General Data Protection Regulation; this means that it must be obtained, used and stored in accordance with the Regulation.

Personal data used as part of an automated biometric recognition system must also comply with the additional requirements in sections 26 to 28 of the Protection of Freedoms Act 2012.

The Protection of Freedoms Act 2012 includes provisions which relate to the use of biometric data in schools, academies and colleges when used as part of an automated biometric recognition system.

Schools and academies must ensure that the parent/carer of each pupil is informed of the intention to use the pupil's biometric data as part of an automated biometric recognition system. Parents/carers must be advised that alternative methods to biometric scanning are available for processing identity if required.

The written consent of the parent/carer or the pupil, where the pupil is deemed to have the capacity to consent (i.e. is over the age of 18 and with the capacity to understand their data rights), must be obtained before the data is taken from the pupil and processed within the biometric recognition system. In no circumstances can a pupil's biometric data be processed without written consent.

Schools and academies must not process the biometric data of a pupil where:

a) the pupil (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data;

b) a parent or pupil has not consented in writing to the processing; or

c) a parent or pupil has objected in writing to such processing, even if another parent has given written consent.

Schools and academies must provide reasonable alternative means of accessing the services to those pupils who will not be using an automated biometric recognition system.

Please also see the DfE's 'Protection of biometric data of children in schools and colleges - July 2022' for further guidance.

2. Biometric Data and Processing

2.1 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 recognition systems can use many kinds of physical or behavioural characteristics such as those listed above.

2.2 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.

2.3 Who Is Able to Give Consent?

The Data Protection Act gives pupils rights over their own data when they are considered to have adequate capacity to understand. Most pupils will reach this level of understanding at around age 13.

However, the Protection of Freedoms Act 2012, which governs the use of biometric data in schools in the UK, has different requirements. Under this Act, **the consent of at least one parent is required to process the biometric data of a child under 18**. If the child or any parent objects, the school cannot process the child's biometric data.

We must notify each parent of a pupil or student under the age of 18 if they wish to take and subsequently use the child's biometric data as part of an automated biometric recognition system.

As long as the child or a parent does not object, the written consent of only one parent will be required for a school or college to process the child's biometric information. A child does not have to object in writing but a parent's objection must be written.

2.4 Alternative to Biometric

The school or academy will provide an alternative to biometric scanning for any parent/pupil objecting to the processing of biometric data.

2.5 Length of Consent

The original written consent is valid until such time as it is withdrawn. However, it can be overridden, at any time either parent/carer or the pupil themselves objects to the processing (subject to the parent's/carer's objection being in writing).

When the student leaves the school or academy, their biometric data will be securely removed from the academy's biometric recognition system.

3. Monitoring and Review of This Policy

The implementation of this Policy is reviewed annually by the school's Senior Leadership Team in consultation with staff and a report is made to the Governance Body.

The school may submit to Cavendish Education proposals for amendments to this Policy.