Data Protection Biometric Data Policy

Last reviewed: February 2021

This policy applies to all schools and operations of the Vale Academy Trust

The following related policies can be found on our Trust/school websites or copies can be obtained from the Trust/school offices upon request:

- Data Protection Policy
- Data Protection Privacy Notice for Job Applicants
- Data Protection Privacy Notice for Pupils, Parent and Carers
- Data Protection Privacy Notice for Staff
- Data Protection Photograph Policy
- Data Protection Data Breach Procedure
- Records Retention Policy

Review period:	24 Months	**Next review:**	December 2022
Owner:	DPO	**Approver:**	Board
Category:	Public	**Type:**	Global

In this document:

- 'the Trust', 'we' and 'our' means the Vale Academy Trust and its schools.
- 'parent' means a parent, carer or other legal guardian, registered as such at a school in the Trust.
- 'adult' means an employee or volunteer in the Trust, or any other adult we ask to participate in an automated biometric recognition system.

Contacts

Queries about this policy should be addressed to our Information Team at InformationTeam@vale-academy.org or 01235 754070.

1. Key points

- When we use **biometric data** we must treat it with appropriate care and comply with the data protection principles as set out in the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR).
- When we use the biometric data of a pupil (under 18) in an **automated biometric recognition system** we must also comply with the requirements under sections 26 to 28 of the Protection of Freedoms Act 2012.
- In our early years and primary settings, we will obtain the written consent of at least one parent before a pupil's biometric data is taken and used, i.e. '**processed',** in an automated biometric recognition system.
- In our secondary and sixth form settings, we will obtain the written consent of both the pupil and at least one parent before the pupil's biometric data is processed in an automated biometric recognition system. Where a pupil does not have sufficient understanding (usually those under the age of 12, or over 12 but with a special educational need which makes understanding their information rights more difficult), the headteacher has discretion to accept only a parental consent.
- For an adult in any setting, we will obtain their written consent before their biometric data is processed in an automated biometric recognition system
- We will not process the biometric data of a pupil where:
    - The pupil (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data;
    - No parent has consented in writing to the processing; or
    - A parent has objected in writing to such processing, even if another parent has given written consent.
- We will not process the biometric data of an adult where they have not provided their written consent.
- We will provide reasonable alternative means of accessing services for those who will not be using an automated biometric recognition system.

2. Definition of terms

Biometric data

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 fingerprint data.

The UK's Information Commissioner considers all biometric information to be *special category data*, which is defined as personal data that needs more protection because it is sensitive. This means that it must be obtained, used and stored in accordance with the special category data conditions set out in the Data Protection Act 2018 and the UK GDPR.

The Protection of Freedoms Act 2012 includes provisions which relate to the use of pupils' biometric data in schools when used as part of an automated biometric recognition system. These provisions are in addition to the requirements of the Data Protection Act 2018 and the UK GDPR.

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. 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.

Biometric recognition systems can use many kinds of physical or behavioural characteristics, such as fingerprints or facial recognition.

Processed/processing biometric data

Processing of biometric data 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:

- recording biometric data, for example taking measurements from a fingerprint via a fingerprint scanner;
- storing biometric information on a database system; or
- 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 individuals.

3. Frequently Asked Questions

What information should the school provide to help someone decide whether to object or give consent?

Any objection or consent must be an informed decision. The school will take steps to ensure that every person being asked to give consent receives full information about the processing of the biometric data, including a description of the kind of system, the nature of the data that will be processed, the purpose of the processing and how the data will be obtained and used. The school will provide pupils with information in a manner that is appropriate to their age and understanding.

In the case of parental consent, what if one parent disagrees with the other?

We will notify each registered parent of a pupil whose biometric information we wish to process. If one parent objects in writing, then the school will not be permitted to take or use that pupil's biometric data.

How will a pupil's right to object work in practice – must they do so in writing?

A pupil is not required to object in writing. An older pupil may be more able to say that they object to the processing of their biometric data. A younger pupil may show reluctance to take part in the physical process of giving the data in other ways. In either case the school will not be permitted to collect or process the data.

Is the school required to ask/tell pupils/parents before introducing an automated biometric recognition system?

The school is not required by law to consult pupils/parents before installing an automated biometric recognition system. However, it is required to notify pupils/parents and secure consent in accordance with this policy before biometric data is obtained or used for the purposes of such a system.

Does the school need to renew consent from pupils/parents every year?

No. The original written consent is valid until such time as it is withdrawn. However, it can be overridden at any time if a pupil or another parent objects to the processing (subject to the parent's objection being in writing). When the pupil leaves the school, their biometric data should be securely removed from the school's biometric recognition system.

Does the school need to notify and obtain consent when it introduces an additional, different type of automated biometric recognition system?

Yes, consent must be informed consent. If, for example, a school has obtained consent for a biometric system for catering services and then later introduces a different biometric system for accessing library services, then the school will have to meet the notification and consent requirements for the new system.

Can consent be withdrawn by a parent?

A parent can withdraw their consent, in writing, at any time. In addition, either parent will be able to object to the processing at any time but they must do so in writing.

When and how can a pupil object?

A pupil can object to the processing of their biometric data or refuse to take part at any stage – i.e. before the processing takes place or at any point after their biometric data has

been obtained and is being used as part of a biometric recognition system. If a pupil objects, the school must not start to process their biometric data or, if they are already doing so, must stop. The pupil does not have to object in writing.

Will consent given on entry to primary or secondary school be valid until the pupil leaves that school?

Yes. Consent will be valid until the pupil leaves the school – subject to any subsequent objection to the processing of the biometric data by the pupil or a written objection from a parent. If any such objection is made, the biometric data should not be processed and the school must remove it from the school's system by secure deletion.

Can the school notify parents, pupils and adults by email, and accept consent via email or electronic form?

Yes – as long as the school is satisfied that the contact details are accurate and the consent received is genuine.

Does the legislation cover other technologies such as palm and iris scanning?

Yes. The legislation covers ***all*** systems that record or use physical or behavioural characteristics for the purpose of identification. This includes systems which use palm, iris or facial recognition, as well as fingerprints.

Is parental notification and consent required under the Protection of Freedoms Act 2012 for the use of photographs and CCTV in schools?

No – not unless the use of photographs and CCTV is for the purposes of an automated biometric recognition system. However, schools and colleges must continue to comply with the requirements in the Data Protection Act 2018 and the UK GDPR when using CCTV for general security purposes or when using photographs of pupils as part of a manual ID system or an automated system that uses barcodes to provide services to pupils. Depending on the activity concerned, consent may be required under the Data Protection Act 2018 and the UK GDPR before personal data is processed.

The Government believes that the Data Protection Act 2018 and the UK GDPR provisions are sufficient to regulate the use of CCTV and photographs for purposes other than automated biometric recognition systems. Photo ID card systems, where a pupil's photo is scanned automatically to provide them with services, would come within the obligations on schools under sections 26 to 28 of the Protection of Freedoms Act 2012, as such systems fall within the definition in that Act of automated biometric recognition systems.

Is parental notification or consent required if a pupil uses or accesses standard commercial sites or software which use face recognition technology?

The provisions in the Protection of Freedoms Act 2012 only cover processing by or on behalf of a school. If a school wishes to use such software for school work or any school business, then the requirement to notify parents and to obtain written consent will apply. However, if a pupil is using this software for their own personal purposes then the provisions do not apply, even if the software is accessed using school equipment.

END