STOUR VALE ACADEMY TRUST

PROTECTION OF BIOMETRIC INFORMATION POLICY

VERSION / DATE	VERSION 1.0 JULY 2023
NEXT VERSION DUE BY	JULY 2024

Contents

1.0 Rationale

The duties and responsibilities placed upon Stour Vale Academy Trust ('the Trust'), comprising member schools and the central team, and contained within the Protection of Freedoms Act 2012, came into effect from 1 September 2013.

This policy explains the requirements for utilising biometric information about pupils for the purposes of using automated biometric recognition systems.

It is important to note that there are no circumstances in which the Trust can lawfully process a pupil's biometric data without having notified each parent of a child and received the necessary consent.

This advice relates to responsibilities specified within the following legislation:

The Protection of Freedoms Act 2012
The UK General Data Protection Regulation
The Data Protection Act 2018

It should be noted that in all settings it is only students who are under 18 who are still regarded as children and who are therefore subject to the provisions set out in the Protection of Freedoms Act 2012.

The UK General Data Protection Regulation and Data Protection Act 2018 requirements apply to all living individuals regardless of age.

This policy forms part of the Trust's evidence demonstrating compliance with Article 5 (1) of the UK General Data Protection Regulation alongside a relevant Data Protection Impact Assessment (DPIA).

2.0 Key Points

- If and when using a pupil's biometric data *(please see below)*, the Trust must treat the data collected with appropriate care and must comply with the data protection principles as set out in Article 5 of the UK General Data Protection Regulation.

- Where the Trust uses the data as part of an automated biometric recognition system *(please see below)*, it must comply with the additional requirements as set out in Sections 26 to 28 of the Protection of Freedoms Act 2012.

- The Trust will ensure that each parent of a child is notified of the Trust's intention to use the child's biometric data *(please see below)* as part of an automated biometric recognition system.

- The written consent of at least one parent must be obtained before the data are taken from the child and used. This applies to all pupils in the Trust under the age of

18. In no circumstances can a child's biometric data be processed without written consent.

- The Trust will not process the biometric data of a pupil 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.

The Trust will provide a reasonable alternative means of accessing the services for those pupils who will not be using an automated biometric recognition system.

3.0 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.

The Information Commissioner considers all biometric information to be special category data as defined by the Data Protection Act 2018. To meet the lawful basis for processing biometric data, the Trust will use explicit consent as outlined in Processing of special categories of personal data Article 9 2 (a) of the Data Protection Act 2018.

Article 4 of the UK General Data Protection Regulation (UK GDPR) defines biometric information as *'personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person which allow or confirm the unique identification of the natural person'*.

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

4.0 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). 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 those listed above *(in the section 'What is biometric data?')*.

5.0 How are biometric technologies used in the Trust?

Biometric technologies in the Trust are used to borrow library books, for cashless canteen systems, vending machines, recording class attendance and payments into schools.

6.0 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.

7.0 The Protection of Freedoms Act 2012

7.1 Notification and Parental Consent

The Trust must notify each parent or any other individual with parental responsibility for a pupil 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 by the Trust to process the child's biometric information. A child does not have to object in writing but a parent's objection must be written.

The Trust will not need to notify a particular parent or seek his or her consent if the Trust is satisfied that:

(a) the parent cannot be found, for example, his or her whereabouts or identity is not known;

(b) the parent lacks the mental capacity to object or to consent;

(c) the welfare of the child requires that a particular parent is not contacted, for example where a child has been separated from an abusive parent who is not to be informed of the child's whereabouts; or

(d) where it is otherwise not reasonably practicable for a particular parent to be notified or his or her consent obtained.

Where neither of the parents of a child can be notified for one of the reasons set out above (which would mean that consent cannot be obtained from either one of them), Section 27 of the Protection of Freedoms Act 2012 sets out who should, in such circumstances, be notified and who can give consent.

If the child is being 'looked after' by a local authority or is accommodated or maintained by a voluntary organisation (i.e. not for profit organisation), the local authority, or as the case may be, the voluntary organisation must be notified and their written consent obtained.

If paragraph (a) does not apply, then notification must be sent to all those caring for the child and written consent must be gained from at least one carer before the child's biometric data can be processed (subject to the child and none of the carers objecting in writing).

There will never be any circumstances in which the Trust can lawfully process a child's biometric information (for the purposes of an automated biometric recognition system) without one of the persons above having given written consent.

When obtaining consent to process the child's biometric information the Trust will ensure that parents are fully informed about what is being processed. This should include: details about the type of biometric information to be taken; how it will be used; the parents' and the pupil's right to refuse or withdraw their consent; and the Trust's duty to provide reasonable alternative arrangements for those pupils whose information cannot be processed.

7.2 The pupil's right to refuse

If a pupil under 18 objects or refuses to participate (or to continue to participate) in activities that involve the processing of their biometric data, the Trust will ensure that the pupil's biometric data are not taken/used as part of a biometric recognition system. The Trust recognises that a pupil's objection overrides any parental consent to the processing.

The Trust will ensure pupils understand that they can object or refuse to allow biometric data to be taken/used.

If the pupil refuses to give their consent then the Trust will make alternative arrangements to access the relevant services.

7.3 Providing alternatives

Reasonable alternative arrangements will be provided for pupils who do not use automated biometric recognition systems either because their parents have refused consent (or parent has objected in writing) or due to the pupil's own refusal to participate in the collection of their biometric data.

The alternative arrangements should ensure that pupils do not suffer any disadvantage or difficulty in accessing services/premises, etc. as a result of their not participating in an automated biometric recognition system.

8.0 Privacy Notice

How biometric data are used, the lawful basis for processing biometric data, and how they are processed and stored by the Trust is included in the Privacy Notice (Pupils) for each member school.

9.0 Data Protection Impact Assessment

The Information Commissioner requires that a Data Protection Impact Assessment is carried out where the Trust plans to process special category information on a large scale and where it processes biometric data.

10.0 Data Protection Act 2018

As a data controller, the Trust must have a lawful basis for processing pupils' personal data (which includes biometric data), in accordance with the Data Protection Act 2018. The provisions in the Protection of Freedoms Act 2012 are in addition to the requirements under the DPA with which the Trust must continue to comply.

The Data Protection Act has six principles with which the Trust complies.

When processing a pupil's personal data, including biometric data for the purposes of an automated recognition system, the Trust must comply with these principles. This means that the Trust is required to:

(a) Store biometric data securely to prevent any unauthorised or unlawful use (Article 5 1 (a) 'lawful, fair and transparent' and Article 5 1 (f) 'integrity and confidentiality')

(b) Not keep biometric data for longer than is needed (Article 5 1 (d) 'accuracy' and Article 5 1 (e) 'storage limitation')

(c) Ensure that biometric data are used only for the purposes for which they are obtained and that such data are not unlawfully disclosed to third parties (Article 5 1 (a) 'lawful, fair and transparent,' Article 5 1 (b) 'purpose limitation' and Article 5 1 (c) 'data minimisation')

11.0 Version control

This policy will be reviewed annually with review and next review dates.

12.0 Further information

For further information, please contact:

YourIG Data Protection Officer Service
Dudley MBC, The Council House, Dudley, DY1 1HF

Email: YourIGDPOService@dudley.gov.uk Tel: 01384 815607

13.0 Additional guidance

This can be found via the following links:

Department for Education's *'Protection of Biometric Information of Children in Schools – Advice for proprietors, governing bodies, head teachers, principals and school staff'*:

ICO guide to data protection for organisations: Guide to data protection | ICO