



# Protection of Biometric Information Policy for Schools

Information Governance (IG) Services.

# YourIG

**Bringing Information Governance solutions to you.**

## Contents

Protection of Biometric Information Policy for Schools.....	3
Rationale .....	3
Key Points .....	4
What is biometric data.....	5
What is an automated biometric recognition system? .....	5
How are biometric technology systems used in school? .....	6
What does processing data mean? .....	6
The Protection of Freedoms Act 2012.....	6
Notification and Parental Consent .....	6
The pupil’s right to refuse.....	8
Providing alternatives.....	9
Privacy Notice.....	9
Notification of intention to process pupil’s biometric information.....	12
Consent form for the use of biometric information.....	15
Version control.....	16
Further Information.....	16
Additional guidance.....	16

## Protection of Biometric Information Policy for Schools

### Rationale

The duties and responsibilities placed upon **Summerhill School** and contained within the Protection of Freedoms Act 2012, came into effect from 1 September 2013.

This policy explains the requirements for when 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 **Summerhill School** 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 Regulations and Data Protection Act 2018 requirements apply to all living individuals regardless of age.

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

## Key Points

- If and when using a pupils' biometric data (*please see below*) Summerhill School 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 Summerhill School 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.
- Summerhill School will ensure that each parent of a child is notified of the schools' 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 is taken from the child and used. This applies to all pupils in Summerhill School under the age of 18. In no circumstances can a child's biometric data be processed without written consent.
- Summerhill School 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.

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

## 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 Summerhill School 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.

## What is a biometric automated 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*).

How are biometric technologies used in school?

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

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.

The Protection of Freedoms Act 2012

### **Notification and Parental Consent**

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

Summerhill School will not need to notify a particular parent or seek his or her consent of the school 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 Summerhill School 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

Summerhill School 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 pupils right to refuse or withdraw their consent; and the school's duty to provide reasonable alternative arrangements for those pupils whose information cannot be processed.

### **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 school will ensure that the pupil's biometric data are not taken/used as part of a biometric recognition system. Summerhill School recognises that a pupil's objection overrides any parental consent to the processing.

Summerhill School 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 Summerhill School will make alternative arrangements to access the relevant services.



## **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.

## Privacy Notice

How biometric data is used, the lawful basis for processing biometric data, how it is processed and stored by the school is included in Summerhill School Privacy Notice (Pupils).

### Data Protection Impact Assessment

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

### Data Protection Act 2018

As a data controller Summerhill School 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 Summerhill School must continue to comply.

The Data Protection Act has six principles with which Summerhill School complies with.

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

#### Version Control

This policy will be evaluated on a regular basis with review and next review dates.

#### Further Information

For further information, please contact [include details of setting/school administrator / data protection officer] – If you have purchased the YourIG Data Protection Officer Service use for DPO:

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

Email: [YourIGDPOService@dudley.gov.uk](mailto:YourIGDPOService@dudley.gov.uk) tel: 01384 815607

## Notification of intention to process pupils' biometric information

### [Actions:

- Read through making sure it is relevant to your educational setting.
- Text in Blue bold [square brackets] is an instruction or needs to be replaced with your school's information.
- BLACK text should be retained
- Relevant text should be transferred onto your schools headed paper
- It is strongly recommended that this is placed on your schools website once complete].

Dear *[name of parent/carer]*

The school wishes to use information about your child as part of an automated (i.e. electronically-operated) recognition system. This is for the purposes of *[specify what purpose is – e.g. catering, library access]*. The information from your child that we wish to use is referred to as 'biometric information' (see next paragraph). Under the Protection of Freedoms Act 2012 (sections 26 to 28), we are required to notify each parent of a child and obtain the written consent of at least one parent before being able to use a child's biometric information for an automated system.

### **Biometric information and how it will be used**

*Biometric information* is information about a person's physical or behavioural characteristics that can be used to identify them, for example, information from their *[fingerprint/iris/palm]*. The school would like to take and use information from your child's *[insert biometric to be used]* and use this information for the purpose of providing your child with *[specify what purpose is]*.

The information will be used as part of an automated biometric recognition system. This system will take measurements of your child's *[insert biometric to be used]* and convert these measurements into a template to be stored on the system. An image of your child's *[insert biometric]* is not stored. The template (i.e. measurements taken from your child's *[insert biometric]*) is what will be used to permit your child to access services.

You should note that the law places specific requirements on schools when using personal information, such as biometric information, about pupils for the purposes of an automated biometric recognition system.

For example:

- (a) the school cannot use the information for any purpose other than those for which it was originally obtained and made known to the parent(s) (i.e. as stated above);
- (b) the school must ensure that the information is stored securely;
- (c) the school must tell you what it intends to do with the information;
- (d) unless the law allows it, the school cannot disclose personal information to another person/body – you should note that the only person/body that the school wishes to share the information with is [*insert any third party with which the information is to be shared e.g. X supplier of biometric systems*]. This is necessary in order to [*say why it needs to be disclosed to the third party*].

### **Providing your consent/objection**

As stated above, in order to be able to use your child's biometric information, the written consent of at least one parent is required. However, consent given by one parent will be overridden if the other parent objects in writing to the use of their child's biometric information. Similarly, if your child objects to this, the school cannot collect or use his/her biometric information for inclusion on the automated recognition system.

You can also object to the proposed processing of your child's biometric information at a later stage or withdraw any consent you have previously given. This means that, if you give consent but later change your mind, you can withdraw this consent. Please note that any consent, withdrawal of consent or objection from a parent must be in writing.

Even if you have consented, your child can object or refuse at any time to their biometric information being taken/used. [*His/her*] objection does not need to be in writing. We would appreciate it if you could discuss this with your child and explain to them that they can object to this if they wish.

The school is also happy to answer any questions you or your child may have.

If you do not wish your child's biometric information to be processed by the school, or your child objects to such processing, the law says that we must provide

reasonable alternative arrangements for children who are not going to use the automated system to [*insert relevant service e.g. access school library*].

If you give consent to the processing of your child's biometric information, please sign, date and return the enclosed consent form to the school.

Please note that when your child leaves the school, or if for some other reason he/she ceases to use the biometric system, his/her biometric data will be securely deleted.

## Version Control

This policy will be evaluated on a regular basis with September 25 as the next review.

## Further information

For further information, please contact [include details of setting/school administrator / data protection officer] – If you have purchased the YourIG Data Protection Officer Service use for DPO:

YourIG Data Protection Officer Service  
Dudley MBC, 3-5 St James's Road, Dudley, DY1 1HZ

Email: [YourIGDPOService@dudley.gov.uk](mailto:YourIGDPOService@dudley.gov.uk) tel: 01384 815607

## 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](#)