Protection of Biometric Information Policy

CONTENTS	Page No
1. Overview of the legislation framework	1
2. Biometric Data	2
3. Consent	3
4. Management of Information	4
Appendix 1 – Draft Parental Consent	6

1. Overview of the legislation framework

The Data Protection Act 2018 and the UK GDPR has updated data protection laws for the digital age, in which an ever-increasing amount of personal data is being held and processed.

The Data Protection Act 20182, UK GDPR3, and the Protection of Freedoms Act 20124 set out how pupils' and students' data (including biometric data) should be processed. Biometric data is special category data5 and must be processed lawfully, fairly and in a transparent way. Schools and colleges should ensure that biometric information is kept safe.

Data controllers determine the purpose or outcome of the processing of the personal data. For the purpose of this guidance, schools and colleges are considered to be Data controllers. Data controllers must comply with and demonstrate compliance with all the data protection principles as well as the other UK GDPR requirements. They are also responsible for the compliance of their processor(s).

Data processors act on behalf of and follow the instructions from the controller regarding the processing of personal data.

UK GDPR requires all data controllers and processors6 to be open and transparent about how and why personal data is used. Data should be processed in line with the following seven UK GDPR principles:

- **lawfulness, fairness and transparency** - Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
- **purpose limitation** - Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- **data minimisation** - Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

- **accuracy** - Personal data shall be accurate and, where necessary, kept up to date.

- **storage limitation** - Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- **integrity and confidentiality** - Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- **accountability** - The controller shall be responsible for and be able to demonstrate compliance with the UK GDPR.

2. Biometric Data

2.1 What is Biometric Data?

Biometric data means personal information resulting from specific technical processing relating to the individual's physical, psychological or behavioural characteristics which allow or confirm the unique identification of that person, such as facial images, iris recognition, voice recognition or fingerprints.

2.2 What is an Automated Biometric Recognition System?

An automated biometric recognition system uses technology to measure an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (i.e. electronically). Biometric systems usually store measurements taken from a person's physical/behavioural characteristics and not images of the characteristics themselves.

2.3 What is Facial recognition?

Facial recognition is the process by which a person can be identified or otherwise recognised from a digital facial image. Cameras are used to capture these images and facial recognition technology software produces a biometric template. Often, the system will then estimate the degree of similarity between two facial templates to identify a match (e.g. to verify someone's identity), or to place a template in a particular category (e.g. age group). This type of technology can be used in a variety of contexts from unlocking our mobile phones, to setting up a bank account online, or passing through passport control.

2.4 What is live facial recognition?

Live facial recognition is different to the facial recognition technology referenced above and is typically deployed in a similar way to traditional CCTV. It is directed towards everyone in a particular area rather than specific individuals. It has the ability to capture the biometric data of all individuals passing within range of the camera automatically and indiscriminately. Their data is collected in real-time and potentially on a mass scale.

2.5 What does processing data mean?

- ‘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 pupil/students’ biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner
- storing pupil/students’ biometric information on a database system
- 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 pupil/students’.

2.6 Data Controller Responsibilities

It is the responsibility of the data controller to identify the additional risks associated with using automated biometric technology by conducting a DPIA ensuring decisions are documented. Controllers should also, be aware of the wider duties placed on them, for example under the Human Rights Act 1998 and Public Sector Equality Act Duty using automated biometric technology. Controllers should also consult with the ICO when making these decisions.

3. Consent

3.1 Who can give consent?

In order to comply with the requirements of the Protection of Freedoms Act 2012, schools and colleges must notify each parent, carer/legal guardian of the child of their intention to process the child’s biometric information, and that the parent may object at any time to the processing of the information. It is important to understand that a child’s biometric information must not be processed unless at least one parent of the child consents, and no parent of the child has withdrawn his or her consent, or otherwise objected, to the information being processed. In addition, a pupil’s or student’s objection or refusal, overrides any parental consent to the processing, therefore any biometric data must not be processed.

The Protection of Freedoms Act 2012 defines a parent to mean “a parent of the child and any individual who is not a parent of the child but who has parental responsibility for the child”. Practically it would be person(s) with parental responsibility for the child, be it birth, adoptive or an appointed body, who a school or college would notify and seek consent from to process personal biometric data. Any one parent could give or withhold consent.

Where a child is looked after and is subject to a care order in favour of the local authority or the local authority provides accommodation for the child within the definition of section 22(1) of the Children Act 1989, a school or college would not be required to notify or seek consent from birth parents.

3.2 Pupils’ right to refuse

If a pupil or student under 18 objects or refuses to participate (or to continue to participate) in activities that involve the processing of their biometric data, the school or college must ensure that the pupil/student’s biometric data is not taken/used as part of a biometric recognition system. A pupil’s or student’s objection or refusal overrides any parental consent to the processing. Section 26 and Section 27 of the Protection of Freedoms Act 2012 makes no reference to a lower age limit in terms of a child’s right to refuse to participate in sharing their biometric data.

Schools and colleges should also take steps to ensure that pupils and students understand that they can object or refuse to allow their biometric data to be taken/used and that, if they do this, the school or college must provide them with an alternative method of accessing relevant services. The steps taken by schools and colleges to inform pupils and students should take account of their age and level of understanding. Parents should also be told of their child's right to object or refuse and be encouraged to discuss this with their child.

3.4 Provision of Alternative Arrangements

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

The alternative arrangements should ensure that pupils and students 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. Likewise, such arrangements should not place any additional burden on parents whose children are not participating in such a system.

4. Management of Information

4.1 Purpose

In line with the purpose limitation principle under Data Protection law, schools and colleges can only store and use the biometric information for the purpose for which it was originally obtained, and parental/child consent given.

4.2 Security

We would expect schools and colleges to carry out the following when considering security of biometric data:

- store biometric data securely to prevent any unauthorised or unlawful use.
- not keep biometric data for longer than it is needed meaning that a school or college should destroy a pupil's/student's biometric data if, for whatever reason, they no longer use the system including when leaving the school or college, where a parent withdraws consent or the pupil/student either objects or withdraws consent.
- 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.

4.3 Protections against unlawful and unauthorised access

It is important that schools and colleges understand their responsibilities, when protecting data. Schools and colleges should:

- identify risks that emerge from the initial assessment.
- assess what can be done to eliminate or reduce areas of medium/high risk and set action plans to do so.
- consider access controls.

- use DPIAs* as a part of their risk identification and mitigation procedures ensuring that the specifics of any flows of personal data between people, systems, organisations and countries have been clearly explained and presented. This will include third party providers of any technology used.

*(The *Data Protection Impact Assessment Article 35 of the UK GDPR introduces a legal requirement to undertake a DPIA for any high-risk processing.)*

HGPS does not currently collect or store pupils' biometric information.

This Policy is based on DfE guidelines – July 2022*

Appendix 1

Parental Notification and Consent Form for the use of Biometric Data

RE: Notification of intention to process pupils' biometric information and consent form

Dear **name of parent**,

I am writing to notify you of the school's wishes to use information about your child as part of an automated (i.e. electronically operated) recognition system.

The purpose of this system is to **[specify what the purpose of the system is, e.g. to facilitate catering transactions to be made using pupils' fingerprints instead of by using cash]**.

The information from your child that we wish to use is referred to as 'biometric information'.

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, e.g. their fingerprint. The school would like to collect and use the following biometric information from your child:

- **[Specify the biometric information you want to collect and process]**

The school would like to use this information for the purpose of providing your child with **[specify the purpose of using the information, e.g. so the child can pay for their school meal using their fingerprint]**.

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

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:

- The school will not 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).

- The school will ensure that the information is stored securely.
- The school will tell you what it intends to do with the information.
- Unless the law allows it, the school will not disclose personal information to another person or body.

Please note, the school has to share the information with the following bodies: • **[Specify any third party with which the information is to be shared, e.g. the supplier of the biometric system]**

This is necessary in order to **[specify why is needs to be disclosed to the third party]**. **Providing your consent/objecting to the use of biometric data**

Under the Protection of Freedoms Act 2012, 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.

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 the use of their biometric information, the school cannot collect or use the information for inclusion on the automated recognition system.

You can also object to the proposed processing of your child's biometric information at any time or withdraw any consent you have previously given. Please note that you must make any consent, withdrawal of consent or objection in writing.

Even if you have given your consent, your child can object or refuse at any time to their biometric information being collected and used – their objection does not need to be in writing.

We would appreciate if you could discuss this with your child and explain to them that theycan object if they want to.

The school is happy to answer any questions you or your child may have – please contact **name of staff member** on **contact details** with any questions.

If you do not wish for your child's biometric information to be used by the school, or your child objects to such processing, the school will provide reasonable alternative arrangements for pupils who are not going to use the automated system to **[insert relevant service, e.g. pay for school meals]**.

Please note that, when your child leaves the school or ceases to use the biometric system, their biometric information will be securely deleted in line with the school's **Records Management Policy**.

Please complete the form below to confirm if you do or do not consent to the collection and use of your child's biometric information and return it to the **school office** by **date**.

Kind regards,
Name
Job role
……

Consent form for the use of biometric information

Please complete this form to confirm whether you provide consent for the school to collect and use the following biometric information relating to your child:

- **[Insert the biometric information the school intends to collect and use]**

This biometric information will be used by the school for the following purpose: •
[Specify the purpose the information will be used for, e.g. catering]

Having read the guidance provided to me by **name of school**, I (please tick your selection):

- **Do** consent to the processing of my child's biometric data
- **Do not** consent to the processing of my child's biometric data

For parents that have provided consent

Please confirm that you have read and understood the following terms:

- I authorise the school to use my child's biometric information for the purpose specified above until either they leave the school or cease to use the system.
- I understand that I can withdraw my consent at any time.
- I understand that, if I wish to withdraw my consent, I must do so in writing and submit this to **address**.
- I understand that once my child ceases to use the biometric system, the school will securely delete my child's biometric information.

I confirm that I have read and understood the terms above

For all parents

NAME OF CHILD	
NAME OF PARENT	
SIGNATURE	
DATE	

Please return this form to the **school office** by **date**.