Grove School

Protection of Biometric Information Policy

This policy has been created in line with the DfE's 'Protection of biometric information of children alongside other relevant legislation. This guidance was last updated July 2022.

https://www.gov.uk/government/publications/protection-of-biometric-information-of-children-in-schools

Grove school Protection of biometric information policy

Approved by governors – autumn 2023

To be reviewed: autumn 2024

Contents:

Statement of intent

Grove school is committed to protecting the personal data of all its pupils and staff, this includes any biometric data we collect and process.

We collect and process biometric data in accordance with relevant legislation and guidance to ensure the data and the rights of individuals are protected. This policy outlines the procedure the Grove school follows when collecting and processing biometric data.

Signed by:

	Headteacher	Date:	
	Chair of governors	Date:	

1. Legal 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 2018[2], UK GDPR[3], and the Protection of Freedoms Act 2012[4] set out how pupils' and students' data (including biometric data) should be processed. Biometric data is special category data[5] 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 processors[6] 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

This guidance sets out the main points schools and colleges should consider before introducing and when using automated biometric technology. Schools and colleges should ensure that they store and process all personal data within the parameters set out in law, and if using automated biometric technology, meet the requirements set out in:

• **Article 6** of the UK GDPR which sets out the six lawful bases for processing data
• **Article 9** of the UK GDPR which sets out the list of special categories of data and conditions for processing

Biometric data is special category data (Article 9(1) UK GDPR) and can only be processed when the data processor has identified both the lawful basis under Article 6 UK GDPR and a separate condition for processing under Article 9 UK GDPR. There are also further conditions that may have to be satisfied under Schedule 1 of the Data Protection Act 2018.

If you are uncertain about any aspect of data protection law or the use of automated biometric technology, you should seek independent advice to make sure that you comply with all necessary legislation.

The Information Commissioner's Office (ICO) https://ico.org.uk/ can also provide advice and support on these issues.

The Protection of Freedoms Act 2012 imposes a requirement on schools and colleges to obtain consent from parents of children under 18 years of age before processing the child's biometric information.

2. Definitions

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, voice recognition or fingerprints.

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.

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.

Facial recognition will often not be appropriate in schools and colleges if other options are available to achieve similar goals, like paying for school lunches. Schools and colleges must establish that facial recognition is both necessary and proportionate within the school and college environment.

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. Live facial recognition is not appropriate in schools or colleges. It would be difficult for a school or college to demonstrate that the use of live facial recognition technology is justified as fair, necessary, proportionate or lawful under Article 6 and Article 9 of the UK GDPR. There is a separate legal regime in the Data Protection Act 2018 which governs the use of biometric data for law enforcement purposes.

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'

Data Controller Responsibilities (Grove School)

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. Roles and responsibilities

3.1. The governing board is responsible for:

- Reviewing this policy on an annual basis.

3.2. The headteacher is responsible for:

- Ensuring the provisions in this policy are implemented consistently.

3.3. The data protection officer (DPO) is responsible for:

- Monitoring the Grove school's compliance with data protection legislation in relation to the use of biometric data.
- Advising on when it is necessary to undertake a data protection impact assessment (DPIA) in relation to the Grove school's biometric system(s).
- Being the first point of contact for the ICO and for individuals whose data is processed by the Grove school and connected third parties.

4. Data protection principles

4.1. The Grove school processes all personal data, including biometric data, in accordance with the key principles set out in the GDPR.

4.2. The Grove school ensures biometric data is:

- Processed lawfully, fairly and in a transparent manner.
- Only collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date, and that reasonable steps are taken to ensure inaccurate information is rectified or erased.
- 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.
- Processed in a manner that ensures appropriate security of the information, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4.3. As the data controller, the Grove school is responsible for being able to demonstrate its compliance with the provisions outlined in the policy.

5. Data protection impact assessments (DPIAs)

5.1. Prior to processing biometric data or implementing a system that involves processing biometric data, a DPIA will be carried out.

5.2. The DPO will oversee and monitor the process of carrying out the DPIA.

5.3. The DPIA will:

- Describe the nature, scope, context and purposes of the processing.
- Assess necessity, proportionality and compliance measures.
- Identify and assess risks to individuals.
- Identify any additional measures to mitigate those risks.

5.4. When assessing levels of risk, the likelihood and the severity of any impact on individuals will be considered.

5.5. If a high risk is identified that cannot be mitigated, the DPO will consult the ICO before the processing of the biometric data begins.

5.6. The ICO will provide the Grove school with a written response (within eight weeks or 14 weeks in complex cases) advising whether the risks are acceptable, or whether the Grove school needs to take further action. In some cases, the ICO may advise the Grove school to not carry out the processing.

5.7. The Grove school will adhere to any advice from the ICO.

6. Notification and consent

Who can give consent?

In order to comply with the requirements of the Protection of Freedoms Act 2012, Grove School 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.

Pupils' and students' 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, Grove School 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.

Grove school 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, Grove school or college must provide them with an alternative method of accessing relevant services. The steps taken by Grove 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.

Once a student is 18 years old they will be considered an adult and as such parental consent is no longer relevant.

7. 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.

8. Data retention

8.1. Biometric data will be managed and retained in line with the Grove school's Records Management Policy.

8.2. If an individual (or a pupil's parent, where relevant) withdraws their consent for their/their child's biometric data to be processed, it will be erased from the Grove school's system.

9. Breaches

9.1. There are appropriate and robust security measures in place to protect the biometric data held by the Grove school. These measures are detailed in the Grove school's Data and E-Security Breach Prevention and Management Plan.

9.2. Any breach to the Grove school's biometric system(s) will be dealt with in accordance with the Data and E-Security Breach Prevention and Management Plan.

10. Monitoring and review

10.1. The governing board will review this policy on an annual basis.

10.2. The next scheduled review date for this policy is autumn 2024.

10.3. Any changes made to this policy will be communicated to all staff, parents and pupils.

11. Management of Information

Purpose

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

Security

Grove School will 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 Grove School should destroy a pupil's/student's biometric data if, for whatever reason, they no longer use the system including when leaving Grove School, 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

Protections against unlawful and unauthorised access

Grove School will:

•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.

Annex A: A Protection of Freedoms Act 2012 and Consent

Notification and Parental Consent:

Grove School 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 Grove 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.

Grove School will not need to notify a particular parent or seek his or her consent if the school or college is satisfied that:

•the parent cannot be found, for example, his or her whereabouts or identity is not known

•the parent lacks the mental capacity to object or to consent

•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

•where it is otherwise not reasonably practicable for a particular parent to be notified or for his or her consent to be obtained

Where neither of the parents of a child can be notified for one of the reasons set out above (which would mean consent cannot be obtained from either 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:

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

The DfE states that they do not see any circumstances in which Grove School can lawfully process a child's biometric information (for the purposes of using an automated biometric recognition system) without one of the persons above having given written consent.

Under the Education (Pupil Registration) Regulations 2006, Grove school is required to keep an admission register that includes the name and address of every person known to the school to be a parent of the child, including non-resident parents. This can be used by schools that wish to notify and seek consent to process a child's biometric information at any point after the enrolment of a child.

Grove School should be alert to the fact that the admission register may, for some reason, not include the details of both parents. Where the name of only one parent is included in the admission register, Grove School must take reasonable steps to ascertain the details of the other parent. For example, the school might ask the parent who is included in the admission register or, where the school is aware of local authority or other agency involvement with the child and its family, may make enquiries with the local authority or other agency.

The school is expected to take reasonable steps to locate a parent before they are able to rely on the exemption in section 27(1)(a) of the Protection of Freedoms Act 2012 (i.e. notification of a parent not required if the parent cannot be found).

Grove school will notify parents that they intend to take and use their child's biometric information as part of an automated biometric recognition system and seek written consent to do so at the same time as obtaining details of parents as part of the enrolment process. In other words, details of both parents would be requested by the school or college for both purposes (enrolment and notification of intention to process biometric information).

Parental Notification and Consent Form for the use of Biometric Data

[The following is suggested text for a notification letter and consent form to parents. You should adapt this text considering your Grove school's specific biometric system(s).]

Address line one
Address line two
Town
County
Postcode
Date

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

Dear **name of parent**,

I am writing to notify you of the Grove 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 Grove 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 Grove 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 Grove 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 Grove schools when using personal information, such as biometric information, about pupils for the purposes of an automated biometric recognition system. For example:

- The Grove 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 Grove school will ensure that the information is stored securely.
- The Grove school will tell you what it intends to do with the information.

- Unless the law allows it, the Grove school will not disclose personal information to another person or body.

Please note, the Grove 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 Grove 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 they can object if they want to.

The Grove 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 Grove school, or your child objects to such processing, the Grove 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 Grove school meals]**.

Please note that, when your child leaves the Grove school or ceases to use the biometric system, their biometric information will be securely erased in line with the Grove 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 **Grove 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 Grove school to collect and use the following biometric information relating to your child:

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

This biometric information will be used by the Grove 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 Grove 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 Grove school to use my child's biometric information for the purpose specified above until either they leave the Grove 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 Grove 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 **Grove school office** by **date**.