Protection of Biometric Information Policy

Signed:

Chair: S. Gribbin

CEO: R. Swindells

Date: 15th October 2026

Review date: October 2027

Contents:

Statement of intent

1. Legal framework
2. Definitions
3. Roles and responsibilities
4. Data protection principles
5. Data protection impact assessments (DPIAs)
6. Notification and consent
7. Alternative arrangements
8. Storage and data retention
9. Security and breaches
10. Monitoring and review

Appendices

A. Parental notification and consent form for the use of biometric data

Collective Vision Trust
Protection of Biometric Information Policy

Statement of intent

This policy applies to the Collective Vision Trust and to all its individual academies.

Collective Vision Trust 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. We will treat the data collected with appropriate care.

This policy outlines the procedure the school follows when collecting and processing biometric data.

Please note: *where this policy uses the term 'headteacher' it refers to the person who is legally registered as headteacher for the school. In some schools this may be the 'Executive Headteacher' unless the policy specifically states the Head of School.*

1. Legal framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Protection of Freedoms Act 2012
- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR)
- Data (Use and Access) Act 2025
- DfE 'Protection of biometric information of children in schools and colleges'
- DfE 'Data protection in schools'

This policy operates in conjunction with all other school and trust policies.

2. Definitions

"**Biometric data**" is personal information, resulting from specific technical processing, about an individual's physical or behavioural characteristics that can be used to identify that person, including their fingerprints, facial shape, retina and iris patterns, hand measurements, and voice. All biometric data is personal data.

An "**automated biometric recognition system**" is a system 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.

"**Processing biometric data**" includes obtaining, recording or holding the data or carrying out any operation on the data including disclosing it, deleting it, organising it or altering it. An automated biometric recognition system processes data when:

- Recording pupils' biometric data, e.g. taking measurements from a fingerprint via a fingerprint scanner.
- Storing pupils' biometric information on a database.
- Using pupils' biometric data as part of an electronic process, e.g. by comparing it with biometric information stored on a database to identify or recognise pupils.

"**Special category data**" is personal data which the UK GDPR says is more sensitive, and so needs more protection. Where biometric data is used for identification purposes, e.g. through keystroke analysis, it is considered special category data.

3. Roles and responsibilities

The Trust Board is responsible for reviewing this policy on an annual basis and:

- Ensuring data protection performance is monitored regularly
- Providing support to the DPO, as necessary

- Ensuring effective network security infrastructure is in place to keep personal data protected.

The CEO is responsible for ensuring the provisions in this policy are implemented consistently across the Trust.

The headteacher is responsible for ensuring the provision in this policy are implemented consistently across the academy and:

- Ensuring the provisions in this policy are implemented consistently
- Ensuring staff receive appropriate training on data protection
- Deciding on how the school processes and uses biometric date.

The data protection officer (DPO) is responsible for:

- Monitoring the school's compliance with data protection legislation in relation to the use of biometric data.
- Identifying, alongside the Technical Manager, the additional risks associated with using automated biometric technology by conducting a data protection impact assessment (DPIA).
- Being the first point of contact for the ICO and for individuals whose data is processed by the school and connected third parties.

The school, as data controller, will remain responsible for compliance where biometric processing is carried out by third-party suppliers or processors on its behalf.

The school will maintain appropriate registration with the ICO and comply with all associated obligations.

4. Data protection principles

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

As the data controller, the school is responsible for being able to demonstrate its compliance with the provisions outlined above.

Information about the school's use of biometric data will be included within the school's privacy notices. This information will explain:

- The purpose for which biometric data is collected and processed.
- The lawful basis under Article 6 UK GDPR and the applicable condition for processing special category data under Article 9 UK GDPR.
- How biometric data will be collected, used, stored and protected.
- Any third parties with whom biometric data may be shared and the reasons for such sharing.
- The period for which biometric data will be retained and the criteria used to determine retention periods.
- The rights available to data subjects in relation to the processing of their biometric data, including the rights to access, rectify, erase, restrict processing, object to processing and lodge a complaint with the ICO.
- How consent may be withdrawn and the arrangements that will be provided where biometric data is no longer processed.

The school will ensure that privacy information relating to biometric data is concise, transparent, easily accessible and written in clear and plain language appropriate to the intended audience.

Before processing biometric data, the school will identify and document:

- An appropriate lawful basis under Article 6 UK GDPR.
- An applicable condition for processing special category data under Article 9 UK GDPR.
- Any additional requirements under Schedule 1 of the Data Protection Act 2018 where relevant.

The school will not use live facial recognition technology. Any proposal to deploy live facial recognition would be considered incompatible with this policy and would require exceptional legal justification.

5. Data protection impact assessments (DPIAs)

Prior to processing biometric data or implementing a system that involves processing biometric data, a DPIA will be carried out. The DPO will oversee and monitor the process of carrying out the DPIA.

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.
- Be reviewed frequently and kept updated.

When assessing levels of risk, the likelihood and the severity of any impact on individuals will be considered. If a high risk is identified that cannot be mitigated, the DPO will consult the ICO before the processing of the biometric data begins.

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

Each DPIA will be treated as a 'living' document to help manage and review the risks of the processing of the biometric data and the measures put in place on an ongoing basis. DPIAs will be reviewed annually or in response to any changes.

6. Notification and consent

Please note: The obligation to obtain consent for the processing of biometric information of children under the age of 18 is not imposed by the Data Protection Act 2018 or the UK GDPR. Instead, the consent requirements for biometric information are imposed by section 26 of the Protection of Freedoms Act 2012.

Where the school uses pupils' biometric data as part of an automated biometric recognition system (e.g. using pupils' fingerprints to receive school dinners instead of paying with cash), the school will comply with the requirements of the Protection of Freedoms Act 2012.

Prior to any biometric recognition system being put in place or processing pupils' biometric data, the school will send pupils' parents a Parental Notification and Consent Form for the use of Biometric Data. Written consent will be sought from at least one parent of the pupil before the school collects or uses a pupil's biometric data.

The name and contact details of pupils' parents will be taken from the school's admission register. Where the name of only one parent is included on the admissions register, the headteacher will consider whether any reasonable steps can or should be taken to ascertain the details of the other parent.

The school does not need to notify a particular parent or seek their consent if it is satisfied that:

- The parent cannot be found, e.g. their whereabouts or identity is not known.
- The parent lacks the mental capacity to object or consent.
- The welfare of the pupil requires that a particular parent is not contacted, e.g. where a pupil has been separated from an abusive parent who must not be informed of the pupil's whereabouts.
- It is otherwise not reasonably practicable for a particular parent to be notified or for their consent to be obtained.

Where neither parent of a pupil can be notified for any of the reasons set out above, consent will be sought from the following individuals or agencies as appropriate:

- If a pupil is being 'looked after' by the LA or is accommodated or maintained by a voluntary organisation, the LA or voluntary organisation will be notified and their written consent obtained.
- If the above does not apply, then notification will be sent to all those caring for the pupil and written consent will be obtained from at least one carer before the pupil's biometric data can be processed.

Notification sent to parents and other appropriate individuals or agencies will include information regarding the following:

- Details about the type of biometric information to be taken
- How the data will be used
- How the data will be stored
- The parent's and the pupil's right to refuse or withdraw their consent
- The school's duty to provide reasonable alternative arrangements for those pupils whose information cannot be processed

The school will not process the biometric data of a pupil under the age of 18 in the following circumstances:

- The pupil (verbally or non-verbally) objects or refuses to participate in the processing of their biometric data
- No parent or carer has consented in writing to the processing
- A parent has objected in writing to such processing, even if another parent has given written consent

Parents and pupils will be made aware that they can object to participation in the school's biometric systems or withdraw their consent at any time, and that if they do this, the school will provide them with an alternative method of accessing the relevant services. Pupils will be informed that they can object or refuse to allow their biometric data to be collected and used. The steps taken by the school to inform pupils will take account of their age and level of understanding. Parents will also be informed of their child's right to object and will be encouraged to discuss this with their child.

Where a pupil or their parents object, any biometric data relating to the pupil that has already been captured will be deleted. If a pupil 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 is not taken or used as part of a biometric recognition system, irrespective of any consent given by the pupil's parent.

Where staff members or other adults use the school's biometric systems, consent will be obtained from them before they use the system. Staff and other adults can object to taking part in the school's biometric systems and can withdraw their consent at any time. Where this happens, any biometric data relating to the individual that has already been captured will be deleted.

Alternative arrangements will be provided to any individual that does not consent to take part in the school's biometric systems, in line with the Alternative arrangements section of this policy.

7. Alternative arrangements

Parents, pupils, staff members and other relevant adults have the right to not take part in the school's biometric systems.

Where an individual objects to taking part in the school's biometric systems, reasonable alternative arrangements will be provided that allow the individual to access the relevant service, e.g. where a biometric system uses pupil's fingerprints to pay for school meals, the pupil will be able to use cash for the transaction instead.

Alternative arrangements will not put the individual at any disadvantage or create difficulty in accessing the relevant service, or result in any additional burden being placed on the individual (and the pupil's parents, where relevant).

8. Storage and data retention

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

The school will only store and process biometric information for the purpose for which it was originally obtained and consent provides.

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

9. Security and breaches

The outcome of the DPIA will be used to identify the security measures that will be put in place to protect any unlawful and/or unauthorised access to the biometric data stored by the school.

Biometric data will not be unlawfully disclosed to third parties.

Security measures will include:

- Appropriate access controls.
- Secure storage arrangements.
- Documented data flows.
- Assessment of third-party supplier security arrangements.
- Periodic review of risks identified through DPIAs.

These security measures and the process that will be followed if there is a breach to the school's biometric systems are outlined in the school's Cyber Security Policy.

10. Monitoring and review

The Trust Board will review this policy on an annual basis.

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

Parental notification and consent form for the use of biometric data

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

Dear 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 facilitate catering transactions to be made using pupils' fingerprints instead of 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:

- Fingerprint

The school would like to use this information so your 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 (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:

- Chartwells Catering
- Civica cashless solution

This is necessary in order to ensure your child is able to pay for their meand and that the systems are maintained.

Providing your consent or objecting to the use of biometric information

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 another 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 they can object if they want to.

The school is happy to answer any questions you or your child may have – please contact Sarah Francis on 01782 568350 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 use a pin number to pay for their meals.

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

Please complete the consent form in the registration pack to give your consent.