**Protection of Biometric Information in School**

1. **Introduction**
2. We are committed to protecting the personal data of all our pupils and staff, this includes any biometric data we collect and process.
3. 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 school follows when collecting and processing biometric data.
4. This policy will be subject to review periodically, but at least biennially, to include consultation with interested parties.

1. **Purpose and Scope of this policy**
2. The purpose of this policy is to set out what biometric data will be collected and used in school and how it is protected.
3. This policy covers how we will have regard to the following legislation and guidance when processing any biometric data:

* Protection of Freedoms Act 2012
* Data Protection Act 2018
* DfE (2018) ‘Protection of biometric information of children in schools and colleges.’

1. The lawful basis for processing biometric data in school is consent.
2. **Relationship with other policies**
3. This policy should be read in conjunction with the following policies:

* Data Protection Policy.
* Records Management and Retention Policy.

#### **Definitions**

*Biometric Data:* Personal information 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, and hand measurements.

*Automated Biometric*

*Recognition System:* 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.

*Processing Biometric*

*Data:* 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:* Certain data that is set out in the Data Protection Act as being classed as sensitive data that requires even more protection than other classes of data. Where biometric data is used for identification purposes it is classed as special category data.

*Parent:* As confirmed by the Freedom of Protection Act 2012, parent means a parent of the child and any individual who is not a parent of the child but who has parental responsibility for the child.

1. **Roles and Responsibilities**
2. The Headteacher is responsible for ensuring the provisions of this policy are implemented consistently.
3. The Data Protection Officer is responsible for monitoring the school’s compliance with data protection legislation in relation to the use of biometric data and advising on when it is necessary to undertake a data protection impact assessment (DPIA) in relation to the school’s biometric system.
4. The Governors are responsible for reviewing this policy on a regular basis and ensuring it is adhered to.
5. **The biometric data we use**
6. We will use fingerprint data on ParentPay. ParentPay is a digital method of payment used within the school. Each child has an account, which parents can load money into using a debit/credit card or will be credited if a child receives free school meals. The child will then be able to pay in school using fingerprint data.
7. **How the biometric data will be collected and used**
8. When a child initially uses the automated biometric recognition system it will take an image of the child’s fingerprint and convert this into a unique code for that child using an algorithm. Each time the child then uses their fingerprint to make a payment the system will recognise that child’s unique code allowing a payment to be taken from that child’s account.
9. The biometric data will not be shared with anyone and will not be used for any other purpose.
10. **Consent**
11. Biometric data is classed as personal data; the controlling and processing of such data is covered by the Data Protection Act 2018.
12. In order to process biometric data we must inform both parents that biometric data is to be collected/processed and obtain consent from at least one parent. This applies to all children aged under 18 years old.
13. School must notify both parents that they are processing biometric data of their child, even if the parents are separated. The only exceptions to this would be:

* if 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 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; or
* where it is otherwise not reasonably practicable for a particular parent to be notified or for his/her consent to be obtained.

1. Where neither of the parents of a child can be notified, for one of the reasons set out in section 7.3 above, meaning neither parent would be able to consent, ‘parent’ is to be read as including each individual who has care of the child. In the case of a looked after child, ‘parent’ is to be read as the local authority looking after that child. In the case of a child being looked after by a voluntary organisation such as foster parents or a children’s home, ‘parent’ means that voluntary organisation. (In accordance with s.28 Protection of Freedoms Act 2012).
2. Parents must be notified of the plan to process their child’s biometric data in

writing and information about such processing must be contained within an

appropriate privacy notice.

1. If a parent objects to the processing of their child’s biometric data, they must do so, in writing. They should be informed of their right to object in writing when they are informed that we are planning to process their child’s biometric data and when consent is being obtained.
2. Parents must be asked to sign a consent form which clearly sets out that they are consenting to the collection and processing of their child’s biometric data.
3. We MUST NOT process a child’s biometric data without obtaining consent from at least one parent.
4. All consent forms should be logged internally on the appropriate system and relevant staff members must be notified of any children who have not consented.
5. A child has the right to refuse to provide their biometric data, even if their parent has consented to this.
6. If a child refuses to provide their biometric data, school cannot force the child to

provide their biometric data.

1. A child does not need to set their refusal out in writing, verbal refusal is enough.
2. Where possible, we should notify parents about the use of biometric data, provide them with the relevant privacy notice and obtain consent for use of biometric data at the point of their child’s admission.
3. Consent only needs to be obtained once, as long as it is clearly stated on the consent form that the consent will last for the duration of the time that the child is

at our school.

1. It must be made clear on the consent form that a parent can withdraw their consent to the processing of biometric data at any time. To withdraw consent, the parent must put confirmation of withdrawal of consent in writing.
2. **What if a parent or child refuses to consent?**
3. As set out in section 7 above, a parent and/or a child has the right to refuse to

consent to the child’s biometric data being collected and processed.

1. If a parent/child objects to the processing of their biometric data, the child should not be disadvantaged in any way and alternative measures should be put in place to ensure that the child still has the same access to provisions, services or premises.
2. If a parent/child objects to the processing of their biometric data, the child should

be allowed to pay for goods/services by another means.

1. **Biometric data and the Data Protection Act 2018**
2. As mentioned, biometric data is personal data and must be processed in accordance with the provisions in the Data Protection Act 2018.
3. Where biometric data is processed for the purpose of uniquely identifying an individual, it is classed as special category data, this means to process we must comply with Article 9 General Data Protection Regulations (‘GDPR’).
4. As consent is required, under the Protection of Freedoms Act 2012, before we can collect and process any biometric data, this will ensure that we are compliant with Article 9 GDPR.
5. All biometric data collected and processed by us will be done securely and will not be shared with anyone externally, apart from the ParentPay automated biometric processing system that we are using to process this personal information.
6. Details of consent obtained and any non-consenting parents/children will be held securely for our internal records only.
7. The biometric data will only be collected and processed for the purposes set out in the letter confirming out intention to use biometric data and the consent form that we ask parents to sign.
8. The biometric data will only be held for the duration of the time the child is a pupil with us, after which it will be securely destroyed/deleted – in accordance with the Records Management and Retention Schedule.
9. **Complaints**

1. Any complaints about the contents of this policy or the way this policy is implemented should be addressed to the headteacher in the first instance. Following which, the school complaints policy should be followed.
2. **Breaches of this policy**

1. Any breach of this policy is initially investigated by the Headteacher and should be referred to the Data Protection Officer, in order for the appropriate action to be taken.
2. **Review**
3. This policy should be reviewed biennially.

Date this Policy was last updated: 17.04.2023

This policy should next be reviewed: 17.04.2025