ISLEWORTH & SYON SCHOOL
FINIS CORONAT OPUS

KEY POLICY

Protection of Biometric Information

DRAFTED BY:	FEF	**STATUS:**	Statutory
APPROVED:	03/2022	**GOV. PANEL:**	Academy Trust
ISSUE:	2	**NEXT REVIEW:**	07/2023

1. Aims

The school aims to:

- Protect the personal data of all of its students and staff. This includes any biometric data that is collected within the school.
- Collect and process biometric data in accordance with relevant legislation and guidance.

2. Biometric Information and How it Should be Used

2.1. LEGAL FRAMEWORK

The legislation that this policy refers to includes the following:

- The Protection of Freedoms Act 2012
- The Data Protection Act 2018
- General Data Protection Regulations (GDPR)
- Protection of Biometric Information of Children in Schools and Colleges (March 2018).

2.2. WHAT IS BIOMETRIC DATA?

2.2.1. 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.

2.2.2. 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.

2.2.3. Biometric recognition systems can use many kinds of physical or behavioural characteristics such as those listed in section 2.2.1 above.

2.3. PROCESSING BIOMETRIC DATA

'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:

- recording pupils' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner;
- storing pupils' biometric information on a database system; or
- 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 students.

2.4. SPECIAL CATEGORY DATA

Personal data, which is considered to be more sensitive, requires more protection. Where biometric data is used for identification purposes, it is considered to be special category data.

3. Roles and Responsibilities

3.1. THE HEADTEACHER

The Headteacher is responsible for:

- Reviewing this policy on an annual basis.
- Ensuring that the provisions in this policy are implemented consistently and rigorously.

3.2. THE DATA PROTECTION OFFICER

The data protection officer is responsible for:

- Monitoring the school's compliance with data protection legislation in relation to the use of biometric data.
- Advising on when a data protection impact assessment should be undertaken.
- Being the first point of contact for the Information Commissioners Office (ICO) and for individuals whose data is processed by the school and connected third parties.

4. Data Protection Principles

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

4.2. Specifically, the school ensures that biometric data is:

- Processed lawfully, fairly and in a transparent manner.
- Only collected for specific purposes and not processed beyond the reason for the collection.
- Limited to the purpose for which it has been collected.
- Accurate and where required updated.
- Rectified or deleted when the data is inaccurate.
- Kept in a form that allows identification of data subjects for no longer than necessary and for the purposes of the collection.
- Processed in a manner that allows for appropriate security, including protection against unlawful processing and the prevention of accidental loss, destruction or damage.

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 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.

5.7. The Trust/Academy will adhere to any advice from the ICO.

6. Providing Consent

6.1. The obligation to provide consent for the processing of biometric data of children under the age of 18 is not imposed by the Data Protection Act 2018 or the GDPR, but by Section 26 of the Protection of Freedoms Act 2012. Where the school uses biometric data as part of an automated biometric recognition system (e.g. using students' fingerprints to purchase refreshments, rather than using cash) the school will comply with the requirements of the Act.

6.2. The school will notify each parent of a student under the age of 18 of they wish their child's biometric data to be collected.

6.3. Written consent will be sought from at least one parent/carer of the student before the collection of biometric data is undertaken.

6.4. The school does not need to notify a particular parent or seek their consent if it 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; or
- Where it is otherwise not reasonably practicable for a particular parent to be notified or for his or her consent to be obtained.

6.5. 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:

- 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.
- If paragraph 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).

6.6. Notification sent to parents should include information about the processing of their child's biometric information that is sufficient to ensure that parents are fully informed about what is being proposed. This should include:

- details about the type of biometric information to be taken;
- how it will be used;
- the parents' and the student's right to refuse or withdraw their consent;
- the school's duty to provide reasonable alternative arrangements for those students whose information cannot be
- processed.

6.7. If a 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 must ensure that the student's biometric data are not taken/used as part of a biometric recognition system. A student's objection or refusal overrides any parental consent to the processing.

6.8. Parents and students can object to participation in the school's biometric system(s) or withdraw their consent at any time. Where this happens, any biometric data relating to the pupil that has already been captured will be deleted.

6.9. Where staff members or other adults use the school`s biometric system(s), consent will be obtained from them before they use the system.

6.10. Staff and other adults can object to taking part in the trust's biometric system(s) 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.

6.11. Alternative arrangements will be provided to any individual that does not consent to take part in the trust`s biometric system(s).

7. Alternative Arrangements

7.1. Where an individual object to taking part in the trust's biometric system(s), 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.

7.2. 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. Data Retention and Destruction

8.1. Biometric data will be retained or destroyed in line with the school's Data Retention and Destruction Policy.

8.2. Where consent is withdrawn, the data will be erased from the school's system.

8.3. When a student leaves the school the data will be erased in line with the Data Retention and Destruction Policy.

9. Monitoring Arrangements

This policy will be reviewed **annually** and it will be made available on the school website.

10. Links with Other Policies

This policy links to the following policies and procedures:

- Data Protection Policy
- Data Retention and Destruction Policy.

11. Further Information

Further information can be found on the following link.

The Department for Education: Protection of Children's Biometric Information in School.