ST PAUL'S ACADEMY

Protection of Biometric Data Policy

'You are God's work of art'
Ephesians 2:10

Approved by: Principal and Governors

Reviewed on: 15th May 2024

Next review due by: September 2026

Contents:

Statement of intent

St Paul's Academy is committed to protecting the personal data of all its learners 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 schools follow when collecting and processing biometric data.

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 fingerscan.

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. Images of the biometric information are not stored. The template (i.e., the measurements taken from the finger) will be used to permit the student/staff member to pay at the canteen till.

Providing your consent/objecting to the use of biometric data

Under the Protection of Freedoms Act 2012, the Academy is required to notify each parent of a child and obtain the written consent of at least one parent before being able to use their biometric information for an automated system.

Written consent will be sought from at least one parent of the learner before the school collects or uses a learner's biometric data.

Written consent will be sought from any staff member before the school collects biometric data.

1. Legal framework

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

- Protection of Freedoms Act 2012
- Data Protection Act 2018
- General Data Protection Regulation (GDPR)
- DfE (2018) 'Protection of biometric information of children in schools and colleges'

1.2. This policy operates in conjunction with the following Academy policies:

- Data Protection Policy
- Records Management Policy

2. Definitions

2.1. **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.

2.2. **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.

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

2.4. **Special category data:** Personal data which the GDPR says is more sensitive, and so

needs more protection – where biometric data is used for identification purposes, it is considered special category data.

3. Roles and responsibilities

3.1. The Academy Board is responsible for:

- Reviewing this policy every two years.

3.2. The Principal is responsible for:

- Ensuring the provisions in this policy are implemented consistently.

3.3. The Data Protection Officer (DPO) is responsible for:

- Monitoring the Academy'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 school's biometric system(s).
- Being the first point of contact for the ICO and for individuals whose data is processed by the school and connected third parties.

4. Data protection principles

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

4.2. The Academy 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 Academy is responsible for being able to demonstrate its compliance with the provisions outlined in 4.2. The GDPR principles are detailed further in the Academy Data Protection Policy. The Academy DPO can be contacted at gdpr@accordio.co.uk

5. Data protection impact assessments (DPIAs)

5.1. Prior to 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 DPO 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 school will adhere to any advice from the ICO.

6. Notification and consent

Please note that 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 GDPR. Instead, the consent requirements for biometric information is imposed by section 26 of the Protection of Freedoms Act 2012.

6.1. Where the schools use learners' biometric data as part of an automated biometric recognition system (e.g. using learners' finger scan to receive school dinners

instead of paying with cash or a PIN, the school will comply with the requirements of the Protection of Freedoms Act 2012.

6.2. Prior to processing a learner's biometric data, the school will send the parents / carers a Academy Learner Consent Form.

6.3. Written consent will be sought from at least one parent of the learner before the school collects or uses a learner's biometric data.

6.4. Notification sent to parents /carers will include information regarding the following:

- How the data will be used
- The parent's and the child's right to refuse or withdraw their consent
- The school's duty to provide reasonable alternative arrangements for those learners whose information cannot be processed

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

- The learner (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

6.6. Parents and learners 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 learner that has already been captured will be deleted.

6.7. If a learner 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 learner's biometric data is not taken or used as part of a biometric recognition system, irrespective of any consent given by the learner's parent(s).

6.8. Learners will be informed that they can object or refuse to allow their biometric data to be collected and used via the Consent Form.

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 school'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 school's biometric system(s), in line with **section 7** of this policy**.**

7. Alternative arrangements

7.1. Learners and staff have the right to not take part in the school's biometric system.

7.2. Where an individual objects to taking part in the school'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 fingerscans to pay for school meals.

7.3. 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 learner's parents, where relevant).

8. Data retention

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

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

9. Breaches

9.1. There are appropriate and robust security measures in place to protect the biometric data held by the school. These measures are detailed in the Academy's ICT Strategic Plan.

9.2. Any breach to the Academy's biometric system(s) will be dealt with by the Academy DPO.