



## Process for Protection of Biometric Information

**Review Date:** June 2027

**Reviewed by:** Data Protection Officer

**Final Approval:** Senior Leadership Team

### **Context**

The Core Values which relate specifically to this policy state that we are working together to form relationships based on:

- **Justice** – everyone is entitled to be treated fairly and to promote the self-esteem of others.
- **Responsibility** – everyone is expected to understand the consequences of their actions.
- **Truth** – everyone is required to be honest and to communicate in a positive manner.

Such values contribute to our common purpose of “Striving for high-quality education with a strong Christian ethos”, and underpin, data practices within the Academy.

### **Intent**

Bishop Stopford School will

- protect the personal data of its students, which includes biometric data
- collect and process biometric data in accordance with relevant legislation and guidance to ensure that the data and individuals' rights are protected.
- The Academy complies with the consent requirements set out in the Protection of Freedoms Act 2012 before collecting or using any biometric data. The UK GDPR principles are detailed further in the Data Protection Policy.

### **Definitions of biometric information and how this will be used**

Biometric information is information about a person's physical or behavioural characteristics which can be used to identify them.

At Bishop Stopford School, CRB Cunningham's ID Management software is used, taking fingerprint measurements to process cashless catering and library access.

This system will take measurements from fingerprints and convert them into a template for storage. An image of the fingerprint is not stored, nor can it be recreated from the template data. The template (i.e. the measurements taken from the fingerprint) is used to identify individuals to permit payments via the cashless catering system and access to library services.

### **Obtaining consent/objection to the use of biometric data**

Under the Protection of Freedoms Act 2012, the Academy is required to notify each parent of a student under 18 years of age and obtain the consent of at least one parent before collecting and processing biometric data for an automated recognition system.

Individuals aged 18 and above may provide their consent.

#### **1. Legal framework**

- 1.1. This process takes full account of all relevant legislation and guidance, including, but not limited to, the following:
  - Protection of Freedoms Act 2012
  - Data Protection Act 2018
  - The United Kingdom General Data Protection Regulation (UK GDPR)

- DfE (2018) 'Protection of biometric information of children in schools and colleges'

1.2. This process operates in conjunction with the following policies:

- Data Protection Policy
- Data Retention Schedule

## **2. Definitions**

**2.1. Automated biometric recognition system:** A system which measures an individual's physical or behavioural characteristics by using equipment which operates 'automatically' (i.e. electronically). Information from the individual is automatically compared with biometric information stored in the system to determine whether there is a match, thereby recognising or identifying the individual.

**2.2. 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 student biometric data, e.g. taking measurements from a fingerprint via a fingerprint scanner;
- storing the biometric information in a database;
- using the biometric data as part of an electronic process, e.g., comparing it with biometric information stored on a database to identify or recognise individuals.

**2.3. Special category data:** Personal data which the UK GDPR categorises as more sensitive, and needs more protection. This encompasses:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data (when used for identification purposes, such as fingerprints or facial recognition)
- Health data (physical or mental health)
- Sex life
- Sexual orientation

## **3 Roles and responsibilities**

3.1. The Academy Trust: reviewing this procedure on an annual basis.

3.2. The Headteacher: ensuring the provisions in this procedure are implemented consistently.

3.3. The Data Protection Lead (DPL):

- Monitoring the academy's compliance with data protection legislation relating to the use of biometric data.
- Being the first point of contact for the Information Commissioner's Office (ICO) and for individuals whose data is processed by the academy and connected third parties.

3.4. The Data Protection Officer (DPO): Advising on when it is necessary to undertake a data protection impact assessment (DPIA) in relation to the academy's biometric system(s).

3.5. Authorised Staff: ensuring biometric data is collected lawfully.

#### **4 Data protection principles**

4.1. The Academy processes all personal data, including biometric data, following the key principles set out in the UK 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 for the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date, and 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 which ensures appropriate security of the information, including protection against unauthorised or unlawful processing and 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, including obtaining and recording the required parental consent for biometric processing. The Academy processes biometric data for identification purposes under Article 9(2)(g) UK GDPR (substantial public interest), together with Schedule 1 Part 2 of the Data Protection Act 2018.

#### **5 Data protection impact assessments (DPIAs)**

5.1. Before 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. The ICO will provide the DPO with a written response (within 8 weeks, or 14 weeks in complex cases) advising whether the risks are acceptable or whether the Academy needs to take further action. In some cases, the ICO may advise the Academy not to carry out the processing. The Academy will adhere to guidance issued by the ICO.

## **6 Notification and consent**

6.1 The obligation to obtain consent for the processing of biometric information of children under the age of 18 arises under section 26 of the Protection of Freedoms Act 2012.

6.2 Where the Academy uses biometric data as part of an automated recognition system, as outlined above, the Academy will comply with the requirements of the Protection of Freedoms Act 2012.

6.3 Before processing a student's biometric data, the Academy will send the parents/carers a consent form.

6.4 Consent **must** be obtained from at least one parent before the Academy collects or uses a student's biometric data.

6.5 Information provided to parents /carers will include information regarding the following:

- how the data will be used;
- the parent and the students' right to refuse or withdraw their consent;
- the Academy's duty to provide reasonable alternative arrangements for those students whose information cannot be processed.

6.6 The Academy **will not** process the biometric data of a student under the age of 18 in the following circumstances:

- the student (verbally or non-verbally) objects to or refuses to participate in the processing of their biometric data;
- no consent in writing from a parent or carer;
- A parent has objected in writing to such processing for their child, even if the other parent has given written consent

6.7 Parents/carers may object to their child's participation in the Academy's biometric system(s), or withdraw their consent at any time. Where this happens, any biometric data relating to the student that has already been captured will be deleted.

6.8 If a student objects to or refuses to participate, or to continue to participate, in activities that involve the processing of their biometric data, the Academy will ensure that the student's biometric data is not taken or used as part of a biometric recognition system, irrespective of any consent given by the parent/carers.

6.9 Alternative arrangements will be provided to any individual who does not consent to take part in the Academy's biometric system(s), in line with Section 7 of this policy.

## **7 Alternative arrangements**

7.1 Where an individual objects to taking part in the Academy's biometric system(s), reasonable alternative arrangements will be provided which allow the individual to access the relevant services. (eg giving their name to purchase food or to borrow books.)

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 student's parents, where relevant).

## **8 Data retention and Retention Schedule**

8.1 Biometric data is managed and retained in line with the Academy's Data

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

## **9 Monitoring & review**

9.1 This process will be reviewed every year or as necessary in response to breaches of processes, or changes in the regulatory environment.