Biometric Data Policy

Title	Biometric Data Policy	
Prepared By	Karen Tyler, Data Manager	Date: January 2020
Checked By	Gerry Cross, Facilities and ICT Manager	Date: September 2021
Last Approved By	Governors' Finance and Premises Committee	Date: September 2023
Version	V01.01	
Document Update	September 2024	

Version History

Version	Date	Amendments
V01.00	January 2020	Approved by Governors
V01.01	September 2023	Reapproved by Governors

"In Christ we flourish"

Introduction

St Gregory's school is committed to protecting the personal data of all its students and staff. This includes biometric data. 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.

Legal Framework

This policy has due regard to the following legislation and guidance:

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

It should be read in conjunction with the following school policies:

- Data Protection Policy
- Records Management and Retention Policy
- Security Breach Prevention and Management 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 students' biometric data, e.g. taking measurements from a fingerprint via a fingerprint scanner;
    - Storing students' biometric information on a database;
    - Using students' biometric data as part of an electronic process, e.g. by comparing it with biometric information stored on a database to identify or recognise students.

- **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.

Roles and responsibilities

The Governing Body is responsible for reviewing this policy on an annual basis.

The Headteacher is responsible for ensuring the provisions in this policy are implemented consistently.

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.
- Being the first point of contact for the ICO and for individuals whose data is processed by the school and connected third parties.

Data protection principles

The school processes all personal data, including biometric data, in accordance with the key principles set out in the 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 it is processed;
- Accurate and, where necessary, kept up-to-date. 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 is 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 above.

Notification and Consent

Where the school uses students' biometric data as part of an automated biometric recognition system, the school will comply with the requirements of the Protection of Freedoms Act 2012. The consent requirements for biometric information are imposed by section 26 of this Act.

Prior to any biometric recognition system being put in place or to processing a students' biometric data, the school will send the students' parents/carers notification of how the data will be collected, stored and processed. The notification will include information regarding the following:

- Details about the type of biometric information to be taken;
- How the data will be used;
- The parent's 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.

Consent will be sought from at least one parent of the student before the school collects or uses a student's biometric data. The name and contact details of the student's parents/carers 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 student requires that a particular parent is not contacted, e.g. where a student has been separated from an abusive parent who must not be informed of the student'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 student can be notified for any of the reasons above, consent will be sought from the following individuals or agencies as appropriate:

- If a student 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 student and written consent will be obtained from at least one carer before the student's biometric data can be processed.

The school 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 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 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 student that has already been captured will be deleted.

If a student objects or refuses to participate, or continue to participate, in activities that involve the processing of their biometric data, the school 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 student's parent(s).

Where staff members or other adults use the school's biometric system(s), 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 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.

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

Alternative arrangements

Parents, students, staff members and other relevant adults have the right to not take part in the school's biometric system(s). 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 students' fingerprints to pay for school meals, the student will be able to use a card 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 (or the student's parents, where relevant).

Data retention

Biometric data will be managed and retained in line with the school's Records Management and Retention Policy. It will be deleted when the student leaves the school.

If an individual (or a student'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.