

ST. PAUL'S CATHOLIC COLLEGE



Protection of Biometric Information Policy

Reviewed	Summer 2023
Approved By	
Next Review Date	Summer 2024

Our Mission at St Paul's

Service to each other: learning to become a self disciplined leader

Teaching that inspires me, that challenges me,
that gives me a lifelong love of learning

Partnership at the heart of our school:
a partnership between school, home and community

Achievement: learn and achieve beyond my expectations within an
internationally-enriched curriculum, using world-class technology, with people
who care

Understanding of me as an individual: staff who know me by name
and help make my experience of school rich and happy

Love and respect experienced through our vibrant Catholic Christian
community

Success: academically, spiritually, morally, socially and beyond the classroom

'Learn to Serve'

***St Paul's is a community of faith echoing St Paul's letter to Timothy where,
as hallmarks of Christian living Paul stresses
"love... service and doing the best that is possible."***

Protection of Biometric Information Policy

1. Introduction and Purpose

- 1.1. St Pauls Catholic College is committed to protecting the personal data of all its pupils and staff, this includes any biometric data we collect and process
- 1.2. As a School we fully adhere to the requirements that any use of automated biometric recognition systems must make full and proper arrangements for notifying parents and obtaining the consent required under the Duties set out in this Policy. There are no circumstances in which a School can lawfully process a pupil's biometric data without having notified each parent of a child and received the necessary consent.
- 1.3. This policy supports our School in our collection and processing of biometric data in accordance with relevant legislation and guidance. This ensures that the data and the rights of individuals are protected. This policy sets out the procedures the School follows when collecting and processing biometric data.

2. Objectives

- 2.1. The objectives of this policy are to ensure that:
 - The handling of all biometric data is fully compliant with all relevant legislation and guidance and reduces risk of any mishandling or data breach in its usage
 - Pupils, their parents and staff are confident and assured that robust processes are in place for handling biometric data
 - Across the school, everyone understands the processes and requirements in use of biometric data prescribed in this policy.

3. Scope

- 3.1. This policy applies to all pupils and staff.

4. Legislation and Regulation

- 4.1. This policy is written in accordance with and 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'
- 4.2. This policy must be read in conjunction with the following school policies:
 - The Data Protection Policy
 - The Information and Records Retention Policy

5. Definitions – Biometric Data

5.1. What is biometric data? ▪

- Biometric data is 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.

5.2. What is an Automated Biometric Recognition System?

- This is a system which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (i.e., electronically). For example, this may include biometric recognition systems for:
 - Registration
 - The library
 - Purchasing food in the canteen
- 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
- In using an Automated Biometric Recognition System we have to not only comply with the GDPR Regulations 2018 but also with the additional requirements set out in Sections 26-28 of the Protection of Freedoms Act 2012.

5.3. How do we process Biometric Data?

An automated biometric recognition system processes data when:

- Recording pupils/staff biometric data, e.g., taking measurements from a fingerprint via a fingerprint scanner.
- Storing pupils/staff biometric information on a database.
- Using pupils/staff biometric data as part of an electronic process, e.g. by comparing it with biometric information stored on a database to identify or recognise pupil

5.4. What is Special Category Data?

- Special category data¹ is 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

6. Data Protection Principles

6.1. The processing of all personal data, including biometric data, is in accordance with the key principles set out in GDPR

6.2. The School will ensure that biometric data is:

- Only collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes
- Processed lawfully, fairly and in a transparent manner
- 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. 6.3. The School is the Data Controller and the school is therefore responsible for being able to show it full compliance with the provisions outlined above.

7. Data Retention

7.1. The school will ensure that biometric data will be used, managed and retained in accordance with all of the requirements set out in the Information Records and Retention Policy.

7.2. If an individual (or a pupils' parent where relevant) withdraw their consent for their or their child's biometric data to be processed, the data will be erased from the school system. A record of the erasure of the data will be date and time stamped.

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

7.4. Staff and other adults may choose to object to taking part in the school's biometric system 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. At deletion there will be date and time stamped record of deletion.

8. Providing Consent for use of Biometric Information

8.1. 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 but is required by provisions in Section 26 of the Protection of Freedoms Act 2012.

8.2. In order to use staff and pupil biometric data as part of an automated biometric recognition system, the school must comply with the provisions set out in the Protection of Freedoms Act 2012.

- 8.3. The school will obtain written consent from at least one parent of the pupil before the school collects or uses any pupil biometric data.
- 8.4. The name and contact details of the pupil's parent/s will be taken from the school's Pupil Admissions Register.
- 8.5. 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.
- 8.6. 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 pupil requires that a particular parent is not contacted, e.g., where a pupil has been separated from an abusive parent who must not be informed of the pupil's whereabouts.
 - It is otherwise not reasonably practicable for a particular parent to be notified or for their consent to be obtained.
- 8.7. Where neither parent of a pupil can be notified for any of the reasons set out above, consent will be sought from the following individuals or agencies as appropriate:
- If a pupil 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 pupil and written consent will be obtained from at least one carer before the pupil's biometric data can be processed.
- 8.8. Notification sent to parents and other appropriate individuals or agencies will include information regarding the following:
- The exact details about the type of biometric information to be taken
 - How the data will be used
 - The parent's and the pupil's right to refuse or withdraw their consent
 - The Trust's duty to provide reasonable alternative arrangements for those pupils whose information cannot be processed
- 8.9. The school will not process the biometric data of a pupil under the age of 18 in the following circumstances:
- The pupil (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

8.10. Parents and pupils can object to participation in a biometric system(s) or withdraw their consent at any time. Where consent is withdrawn any biometric data relating to the pupil that has already been captured will be deleted. A record of the erasure of the data will be date and time stamped.

8.11. If a pupil objects or refuses to participate, or to continue to participate, in activities that involve the processing of their biometric data, the Trust will ensure that the pupil's biometric data is not taken or used as part of a biometric recognition system, irrespective of any consent given by the pupil's parent(s).

9. Reasonable alternatives to the use of biometric data.

9.1. The use of biometric data will always be with explicit consent and meet requirements laid out in this policy. There must also be available an alternative, which is a genuine and non-prejudicial alternative.

9.2. The School will ensure that parents, pupils, staff members and other relevant adults have the right to not take part in the schools biometric system(s) by having access to an alternative.

9.3. For example, our cashless catering system for pupils can give pupils a PIN code to use instead of requiring use biometric data for scanning when purchasing refreshments from the canteen.