ST JAMES'
CATHOLIC HIGH SCHOOL

Protection of biometric information of children in schools

Date of Adoption:	March 23
Date of Review:	September 24 (SMBC)

St James' Mission Statement:

*To ensure everyone within our school **family** achieves their full potential, to encourage learning anddevelopment through **faith**, and to strive for **excellence***

Rationale:

We believe everyone has the right to his own property, both intellectual and real. Data protection measures must respect and uphold this right. We recognise and comply with our responsibility to safeguard information in compliance with the General Data Protection Regulation and Data Protection Act 2018. However, as part of a Catholic school community, we have an additional responsibility to recognise that we are 'data stewards' not 'data owners'. We collect, store, handle and share data, only for purposes that uphold the inherent dignity and rights of the human person and the interests of the Common Good.

Contents

1. Introduction

St James' Catholic High School is committed to protecting the personal data of all its pupils and staff. This includes any biometric data the school collects and uses. Biometric data is processed in accordance with relevant legislation and guidance to ensure the data and the rights of individuals are protected. This policy outlines the procedures the school follows when collecting and processing biometric data.

2. Legal Framework

This policy reflects all relevant legislation and guidance including, but not limited to, the following:

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

This policy should also be read in conjunction with the school's Data Protection Policy: https://www.stjamescheadle.co.uk/wp-content/uploads/07.-Data-Protection-Policy-Website-Juliet-Doherty-LS.pdf

3. Definitions

Biometric Data: Personal information about an individual's physical or behavioural characteristics which can be used to identify that person, such as 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 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 pupils.

Special category data: Personal data which the UK GDPR says is more sensitive, and so needs more protection. Where biometric data is used for identification purposes, it is considered special category data.

4. Responsibilities

The School Business Manager is responsible for ensuring the provisions of this policy are implemented throughout the school and ensuring any risks associated with the processing of biometric data are identified and mitigated.

Staff are responsible for recognising the use of biometric data and ensuring appropriate advice is requested from the **Data Protection Officer** to ensure any processing is fair and legal.

5. The Data Protection Act 2018 and UK GDPR

As data controllers, schools must process pupils' personal data (which includes biometric data), in accordance with the UK GDPR / Data Protection Act 2018 (DPA). The provisions in the Protection of Freedoms Act 2012 are in addition to the requirements under the DPA with which schools must continue to comply.

The DPA sets out key data protection principles with which all data controllers must comply. This ensures 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.

As the data controller, the school is responsible for being able to demonstrate its compliance with the provisions outlined above.

6. Data Protection Impact Assessment

The Data Protection Act 2018 requires an organisation to ensure a Data Protection Impact Assessment (DPIA) is carried out for any high-risk processing.

The DPIA is a mechanism for identifying and examining the impact of new initiatives and putting in place measures to minimise or reduce risks during the design stages of a process and throughout the lifecycle of the initiative. Prior to any new processing of biometric data or implementing a system that involves processing biometric data, a DPIA will be carried out.

The school's DPO will oversee and monitor the process of carrying out the DPIA.

7. Lawful Basis

Biometric data constitutes as special category data and the processing of such data is subject to the requirements of the UK General Data Protection Regulations (GDPR). To comply with these regulations **St James' Catholic High School** obtain parents' consent so that we may process biometric data. Where a pupil is aged 12 or over, the school will also obtain the pupil's consent.

8. Obtaining consent

Alongside data protection legislation, there is also an obligation to obtain consent for the processing of biometric information of children under the age of 18, under provisions in Section 26 of the Protection of Freedoms Act 2012.

St James' Catholic High School will notify each parent of a pupil under the age of 18 if it is to use the pupil's biometric data as part of an automated biometric recognition system.

As long as the pupil or a parent does not object, the written consent of only one parent is required for a school to process the child's biometric information. A pupil does not have to object in writing but a parent's objection must be written.

The school does not need to notify a particular parent or seek his or her consent if the school 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 pupil requires that a particular parent is not contacted,
- for example where a pupil has been separated from an abusive parent who is not to be informed of the pupil'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.

Where neither of the parents of a pupil can be notified for one of the reasons set out above, consent will be sought from one of the following (as set out by section 27 of the Protection of Freedoms Act 2012):

- if the pupil is being 'looked after' by a local authority or is accommodated or maintained by a voluntary organisation the local authority, 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 must be gained from at least one carer before the pupil's biometric data can be processed.

Notification sent to parents will outline the following information about the processing of the pupil's biometric information to ensure that parents are fully informed about what is being proposed. This includes:

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

9. Alternative Arrangements

Parents, pupils, staff members and other relevant adults have the right to not take part in the school's biometric system(s). Where an objection is received the school will put in reasonable alternative arrangements to ensure the individual is able 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.

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).

10. Data Retention

Biometric data will be managed and retained in line with the school's Records Retention Schedule. For more information please contact: **SBM@stjamescheadle.co.uk**.

If consent for biometric data processing is withdrawn by the individual or their parents, the data will be deleted from the relevant system.

11. Further Information

Department for Education's 'Protection of Biometric Information of Children in schools – Advice for proprietors, governing bodies, head teachers, principals and school staff: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1092507/Biometrics_Guidance_July_2022.pdf

ICO guidance on data protection for education establishments: https://ico.org.uk/your-data-matters/schools/