

PROTECTION OF BIOMETRIC INFORMATION

OUR TRUST PRAYER

Heavenly Father,
Let peace, friendship and love grow in our schools.
Send the Holy Spirit to give
excellence to our learning,
love to our actions and
joy to our worship.
Guide us to help others,
so that we may all
Learn, Love and Achieve, Together with Jesus.
Amen

Key Points

- Schools that use pupil/student biometric data must treat the data collected with appropriate care and must comply with the data protection principles as set out in the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR).
- Where the data is used as part of an automated biometric recognition system schools and colleges must also comply with the additional requirements in sections 26 to 28 of the Protection of Freedoms Act 2012.
- Schools must ensure that each parent/carer of a child is notified of the school's intention to use the child's biometric data as part of an automated biometric recognition system.
- The **written consent of at least one parent/carer** must be obtained before the data is taken from the pupil/student and used. This applies to all pupils/students in schools **under the age of 18**. In no circumstances can a child's biometric data be processed without written consent.
- Schools **must not process the biometric data of a pupil/student (under 18 years of age) where:**
 - a) the pupil/student (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data;
 - b) no parent/carer has consented in writing to the processing; or
 - c) a parent/carer has objected in writing to such processing, even if another parent/carer has given written consent.
- Schools must provide reasonable alternative means of accessing services for those pupils/students who will not be using an automated biometric recognition system.

Biometric Information

The school must seek consent in order to use information about pupils/students as part of an automated (i.e. electronically operated) recognition system. The special category information is referred to as 'biometric information'.

Biometric information in school is used for the purposes of library and dinner menu access. At St James we do not use Biometric information at present.

Under the Protection of Freedoms Act 2012 (sections 26 to 28), school is required to notify parents/carers and obtain the written consent of at least one parent/carer before being able to use a child's biometric information for an automated system.

The Data Protection Impact Assessment (DPIA)

Article 35 of the UK GDPR introduces a legal requirement to undertake a DPIA for any high-risk processing. Using biometric information is regarded as high-risk processing. A DPIA is designed to describe the data processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them.

DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the UK GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the regulations.

DPIAs should not be viewed as a one-off exercise. A DPIA is a 'living' document and process to help schools manage and review the risks of the processing and the measures put in place on an ongoing basis.

School will need to review its DPIA annually or when there are any changes. As per Article 36 of the UK GDPR, you must consult with the ICO if your DPIA identifies a high risk and you cannot put in place measures to reduce it, in these instances you cannot begin processing until the Trust's Data Protection Officer has consulted with the Information Commissioners Office.

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 (for example, information from their fingerprint). The school will seek consent to take and use pupil/student fingerprint data and use this information for the purpose of providing them with library or dinner menu access. At St James we do not use Biometric information at present.

The information will be used as part of an automated biometric recognition system. This system will take measurements of a fingerprint and convert these measurements into a template to be stored on the system. An image of the fingerprint is not stored. The template (i.e. measurements taken from the fingerprint) is what will be used to permit a pupil/student access to services.

NOTE: the law places specific requirements on schools when using personal information, such as biometric information, about pupils/students for the purposes of an automated biometric recognition system.

For example:

- a. the school cannot use the information for any purpose other than those for which it was originally obtained and made known to the parents/carers [Pupil Privacy Notice](#);
- b. the school must ensure that the information is stored securely (the school has a Data Protection Policy that outlines the security levels in place [Data Protection Policy](#));
- c. the school must tell you what it intends to do with the information (the school asks parents/carers to complete a consent form which outlines how the information will be used);
- d. unless the law allows it, the school cannot disclose personal information to another person/body – you should note that the only person/body that the school wishes to share the information with is the supplier of the Biometric system. At Present St James does not use Biometric systems. This is necessary in order to say why it needs to be disclosed to the third party, eg to support the system software on the secure database.

Providing consent/objecting

In order to be able to use a child's biometric information, the written consent of at least one parent/carer is required. However, consent given by one parent/carer will be overridden if the other parent/carer objects in writing to the use of their child's biometric information. Similarly, if a child objects to this, the school cannot collect or use their biometric information for inclusion on the automated recognition system.

A parent/carer can also object to the proposed processing of their child's biometric information at a later stage or withdraw any consent previously given. This means that if a parent/carer gives consent but later changes their mind, they can withdraw this consent. Please note that any consent, withdrawal of consent or objection from a parent/carer must be in writing.

Even if a parent/carer has consented, their child can object or refuse at any time to their biometric information being taken/used. Their objection does not need to be in writing. Parents/carers should be encouraged to discuss this with their child and explain to them that they can object to this if they wish.

If a parent/carer does not wish their child's biometric information to be processed by the school, or their child objects to such processing, the law says that school must provide reasonable alternative arrangements for children who are not going to use the automated system to access dinner menus or Library services. We do not use biometric at the moment at St James. The alternative arrangements should ensure that pupils and students do not suffer any disadvantage or difficulty in accessing services/premises etc as a result of their not participating in an automated biometric recognition system. Likewise, such arrangements should not place any additional burden on parents whose children are not participating in such a system.

A consent form must be provided to all parents/carers (either separately or collectively with other data processing where consent is required {eg use of photos on websites}) and must include a section regarding biometric information. The school's Pupil/Student Privacy Notice must also be made available and uploaded to the school's website.

Please note that when a child leaves the school, or if for some other reason they cease to use the biometric system, their biometric data will be securely deleted.

More detailed information regarding the Protection of Freedoms Act 2012 and Consent can be found in Appendix 1.

APPENDIX 1 - Protection of Freedoms Act 2012 and Consent

Notification and Parental Consent

Schools must notify each parent¹ of a pupil or student under the age of 18 if they wish to take and subsequently use the child's biometric data as part of an automated biometric recognition system. As long as the child or a parent does not object, the written consent of only one parent will be required for a school or college to process the child's biometric information. A child does not have to object in writing but a parent's objection must be written. School will 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 capacity² to object or to consent
- the welfare of the child requires that a particular parent is not contacted, for example where a child has been separated from an abusive parent who is not to be informed of the child's whereabouts
- 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 child can be notified for one of the reasons set out above (which would mean consent cannot be obtained from either of them), section 27 of the Protection of Freedoms Act 2012 sets out who should, in such circumstances, be notified and who can give consent:

(a) if the child is being 'looked after' by a local authority³ or is accommodated or maintained by a voluntary organisation (i.e. a not-for profit organisation), the local authority, or as the case may be, the voluntary organisation must be notified and their written consent obtained

(b) if paragraph (a) above does not apply, then notification must be sent to all those caring for the child and written consent must be gained from at least one carer before the child's biometric data can be processed (subject to the child and none of the carers objecting in writing).

We do not foresee any circumstances in which a school can lawfully process a child's biometric information (for the purposes of using an automated biometric recognition system) without one of the persons above having given written consent.

Under the Education (Pupil Registration) Regulations 2006, schools are required to keep an admission register that includes the name and address of every person known to the school to be a parent of the child, including non-resident parents. This can be used by schools that wish to notify and seek consent to process a

¹ The parents of a child include not only the biological mother or father (or the adoptive parents) but any other individual with parental responsibility for the child. Part 1 of the Children Act 1989 sets out who has parental responsibility and what this means.

² Within the meaning of the Mental Capacity Act 2005.

³ For example, the child is subject to a care order in favour of the local authority or the local authority provides accommodation for the child – see section 22 of the Children Act 1989 for the definition of 'looked after' child.

child's biometric information at any point after the enrolment of a child. Schools should be alert to the fact that the admission register may, for some reason, not include the details of both parents. Where the name of only one parent is included in the admission register, schools must take reasonable steps to ascertain the details of the other parent. For example, the school might ask the parent who is included in the admission register or, where the school is aware of local authority or other agency involvement with the child and its family, may make enquiries with the local authority or other agency.

Schools are not expected to engage the services of 'people tracer' or detective agencies but are expected to take reasonable steps to locate a parent before they are able to rely on the exemption in section 27(1)(a) of the Protection of Freedoms Act 2012 (i.e. notification of a parent not required if the parent cannot be found).

An option would be for schools to notify parents that they intend to take and use their child's biometric information as part of an automated biometric recognition system and seek written consent to do so at the same time as obtaining details of parents as part of the enrolment process. In other words, details of both parents would be requested by the school or college for both purposes (enrolment and notification of intention to process biometric information).

Notification sent to parents should include information about the processing of their child's biometric information that is sufficient to ensure that parents are fully informed about what is being proposed. This should include details about the type of biometric information to be taken; how it will be used; the parents' and the pupil's or student's right to refuse or withdraw their consent; and the school's duty to provide reasonable alternative arrangements for those pupils whose information cannot be processed.