Data Protection Policy

St. John's Catholic Comprehensive School

Excellence for All

Service to Others

Inspired by Christ

Date of last review:	May 2026	**Date of next review:**	May 2027
Owner:	Data Protection Officer	**Quality Assures:**	Associate Headteacher
Approval:	Full Governing Body Panel		

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the United Kingdom General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA). It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

Scope of the Policy

Personal information is any information that relates to a living individual who can be identified from the information. This includes any expression of opinion about an individual and intentions towards an individual. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings.

The School collects a large amount of personal data every year including: student records, names and addresses, examination marks, references, as well as the many different types of research data used by the School. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

St John's Catholic Comprehensive school currently operates a Biometric Cashless Catering Facility which requires the use of Biometric data. For further information on biometric data please see Appendix 1.

The Principles

The principles set out in the GDPR must be adhered to when processing personal data:

1. Personal data must be processed lawfully, fairly and in a transparent manner (**lawfulness, fairness and transparency**)
2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (**purpose limitation**)
3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed (**data minimisation**)
4. Personal data shall be accurate and where necessary kept up to date and every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay (**accuracy**).
5. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data is processed (**storage limitation**)
6. Appropriate technical and organisational measures shall be taken to safeguard the rights and freedoms of the data subject and to ensure that personal information are processed in a manner that ensures appropriate security of the personal data and protects against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (**integrity and confidentiality**).

Lawful Basis for processing personal information

Before the school conducts any processing activity for the first time, and then regularly afterwards, the purpose(s) for the processing activity and the most appropriate lawful basis (or bases) for that processing must be decided:

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the school

- Processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract

- Processing is necessary for compliance with a legal obligation to which the data controller is subject

- Processing is necessary in order to protect the vital interests of the data subject or of another natural person

- Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party

- The data subject has given consent to the processing of his or her data for one or more specific purposes. Agreement must be indicated clearly either by a statement or positive action to the processing.

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be reviewed if personal data is intended to be processed for a different and incompatible purpose which was not disclosed when the data subject first gave consent.

Sensitive Personal Information

Sensitive personal information is data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or orientation or is genetic or biometric data which uniquely identifies a natural person.

Sensitive personal information will only be processed if:

- There is a lawful basis for doing so as identified in the previous section
- One of the special conditions for processing sensitive personal information applies:
    - (a) the individual ('data subject') has given explicit consent
    - (b) the processing is necessary for the purposes of exercising the employment law rights or obligations of the school or the data subject
    - (c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent
    - (d) the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim
    - (e) the processing relates to personal data which are manifestly made public by the data subject
    - (f) the processing is necessary for the establishment, exercise or defence of legal claims
    - (g) the processing is necessary for reasons of substantial public interest
    - (h) the processing is necessary for purposes of preventative or occupational medicine, for the assessment of the working capacity of the data subject, the provision of social care and the management of social care systems or services
    - (i) the processing is necessary for reasons of public interest in the area of public health.

Sensitive personal information will not be processed until an assessment has been made of the proposed processing as to whether it complies with the criteria above.

Responsibilities

1.1 The school must:

Manage and process personal data properly
Protect the individual's right to privacy

Provide an individual with access to all personal data held on them.

1.2 The school has a legal responsibility to comply with the Act. The school, as a corporate body, and is named as the Data Controller under the Act.

Data Controllers are people or organisations who hold and use personal information. They decide how and why the information is used and have a responsibility to establish workplace practices and policies that are in line with the Act.

1.3 The school is required to notify the Information Commissioner of the processing of personal data.

1.4 Every member of staff who holds personal information has to comply with the Act when managing that information.

1.5 The school is committed to maintaining the principles at all times. This means that the school will:

- inform Data Subjects why they need their personal information, how they will use it and with whom it may be shared. This is known as a Privacy Notice.
- check the quality and accuracy of the information held
- apply records management policies and procedures to ensure that information is not held for longer than is necessary
- ensure that when information is authorised for disposal it is disposed of appropriately
- ensure appropriate security measures are in place to safeguard personal information whether that is held in paper files or on a computer system
- only share personal information with others when it is necessary and legally appropriate to do so
- set out clear procedures for responding to requests for access to personal information known as subject access in the Data Protection Act

- train all staff so that they are aware of their responsibilities and of the school's relevant policies and procedures

Data breaches

A data breach may take many different forms:

- Loss or theft of data or equipment on which personal information is stored
- Unauthorised access to or use of personal information either by a member of staff or third party
- Loss of data resulting from an equipment or systems (including hardware or software) failure
- Human error, such as accidental deletion or alteration of data
- Unforeseen circumstances, such as a fire or flood
- Deliberate attacks on IT systems, such as hacking, viruses or phishing scams
- Blagging offences where information is obtained by deceiving the organisation which holds it

The school must report a data breach to the Information Commissioner's Office (ICO) without undue delay and where possible within 72 hours, if the breach is likely to result in a risk to the rights and freedoms of individuals. The school must also notify the affected individuals if the breach is likely to result in a high risk to their rights and freedoms.

This policy will be reviewed every year and updated as necessary to reflect best practice or amendments made to the GDPR or DPA.

APPENDIX 1

BIOMETRIC DATA PROCESSING

(A) What is biometric data?

1. Biometric data means personal information about an individual's physical or behavioral characteristics that can be used to identify that person; this can include their fingerprints, facial shape, retina and iris patterns, and hand measurements.

2. The Information Commissioner considers all biometric information to be personal data as defined by the Data Protection Act 2018; this means that it must be obtained, used and stored in accordance with the Act.

3. The Protection of Freedoms Act includes provisions which relate to the use of biometric data in schools and colleges when used as part of an automated biometric recognition system. These provisions are in addition to the requirements of the Data Protection Act 2018.

4. (See the Protection of Freedoms Act 2012 below).

(B) What is an automated biometric recognition system?

1. An automated biometric recognition system uses technology 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.

2. Biometric recognition systems can use many kinds of physical or behavioral characteristics such as those listed in (A) 1 above.

(C) What does processing data mean?

'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:

(i) recording pupils' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner;
(ii) 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.

THE PROTECTION OF FREEDOMS ACT 2012

Notification and Parental Consent - What the Law Says:

(1) Schools and colleges must notify each parent of a pupil 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.

(2) 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.

(3) Schools and colleges will not need to notify a particular parent or seek his or her consent if the school or college is satisfied that: a. the parent cannot be found, for example, his or her whereabouts or identity is not known; b. the parent lacks the mental capacity to object or to consent; c. 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; or d. where it is otherwise not reasonably practicable for a particular parent to be notified or for his or her consent to be obtained.

(4) 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 authority 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 consent, written consent obtained. (b) If paragraph (a) above does not apply, then notification must be sent to 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. Within the meaning of the Mental Capacity Act 2005 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. 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).

(5) There will never be any circumstances in which a school or college 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.

(6) Under the Education (Pupil Registration) Regulations 2024, schools are required to keep an admissions 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. Schools that wish to notify and seek consent to process a child's biometric information at any point after the enrolment of a child should have contact details for most parents in the admission register.

(7) 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 should consider whether any reasonable steps can or should be taken 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 and colleges 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 (i.e.; notification of a parent not required if the parent cannot be found).

(8) An option would be for schools and colleges 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).

(9) 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 parent's and the pupil'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.

(10) St John's Catholic Comprehensive school currently operates a Biometric Cashless Catering Facility which requires the use of Biometric data.

<u>The Pupil's Right to Refuse – What the Law Says:</u>

(1) If a pupil under 18 objects or refuses to participate (or to continue to participate) in activities that involve the processing of their biometric data, the school or college must ensure that the pupil's biometric data are not taken/used as part of a biometric recognition system. A pupil's objection or refusal overrides any parental consent to the processing. Also note:

(2) Schools and colleges should take steps to ensure that pupils understand that they can object or refuse to allow their biometric data to be taken/used and that, if they do this, the school or college will have to provide them with an alternative method of accessing relevant services. The steps taken by schools and colleges to inform pupils should take account of their age and level of understanding. Parents should also be told of their child's right to object or refuse and be encouraged to discuss this with their child.

(3) In addition to the required actions for notification and obtaining consent, schools may wish to include information in their privacy notices and explain how biometric data are to be processed and stored by the school.

Providing Alternatives – What the Law Says:

(1) Reasonable alternative arrangements must be provided for pupils who do not use automated biometric recognition systems either because their parents have refused consent (or a parent has objected in writing) or due to the pupil's own refusal to participate in the collection of their biometric data.

(2) The alternative arrangements should ensure that pupils 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. (The Data Protection Act 2018)

(3) As data controllers, schools and colleges must process pupils' personal data (which includes biometric data), in accordance with the 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 and colleges must continue to comply.

(4) When processing a pupil's personal data, including biometric data for the purposes of an automated biometric recognition system, schools and colleges must comply with these principles. This means, for example, that they are required to; a. Store biometric data securely to prevent any unauthorised or unlawful use. b. Not keep biometric data for longer than it is needed meaning that a school or college must destroy a child's biometric data if, for whatever reason, the child no longer uses the system including when he or she leaves the school or college or where a parent withdraws consent or the child objects. c. Ensure that biometric data is used only for the purposes for which they are obtained and that such data is not unlawfully disclosed to third parties.