St John Henry Newman Catholic Primary School

Privacy Notice

Approved: September 2026
Next Review Date: September 2028

1. Introduction

St John Henry Newman Catholic Primary School is committed to protecting the privacy of the personal information we hold.

We collect and use personal data to enable us to educate and safeguard pupils, support families, employ staff, manage the school effectively and meet our legal responsibilities.

Data protection law requires us to be transparent about how we collect and use personal information.

This Privacy Notice explains:

- what personal information we collect;
- where we obtain it from;
- why we use it;
- the legal reasons for using it;
- who we share it with;
- how we protect it;
- how long we keep it; and
- the rights individuals have over their information.

This notice applies to personal information processed by St John Henry Newman Catholic Primary School.

It should be read alongside our:

- Data Protection Policy;
- Data Retention Policy and Data Retention Schedule;
- Parent/Carer Privacy Notice;
- Children's Privacy Notice;
- Visitor Privacy Notice;
- Staff privacy information; and
- other relevant school policies and procedures.

The school will review its privacy information at least annually and whenever there is a significant change to the way personal data is processed. This reflects current Department for Education guidance.

2. Who are we?

St John Henry Newman Catholic Primary School is a voluntary-aided maintained Catholic primary school in Peterborough.

For the purposes of data protection legislation, the school is the data controller for the personal data it processes.

Our school details are:

St John Henry Newman Catholic Primary School
Aqua Drive
Hampton Water
Peterborough
PE7 8QL
Telephone: 01733 304533
Email: office@stjhn.org.uk

The school is responsible for ensuring that personal data is handled lawfully, fairly, securely and transparently.

3. Our Data Protection Officer

The school has appointed an independent Data Protection Officer (DPO).

The DPO advises the school and monitors compliance with data protection legislation.

Data Protection Officer
The ICT Service
Email: dpo@theictservice.org.uk
Telephone: 0300 300 0000, option 1

Address:
Speke House
17 Compass Point Business Park
Stocks Bridge Way
St Ives
Cambridgeshire
PE27 5JL
The DPO can be contacted about:

- questions concerning this Privacy Notice;
- data protection rights;
- concerns about how information is being used;
- Subject Access Requests;
- personal data breaches;
- Data Protection Impact Assessments; and
- other data protection matters.

4. What personal data do we collect?
The personal information we collect will depend on the individual's relationship with the school.
It may include:
Pupils and children

- name;
- date of birth;
- address;
- unique pupil numbers;
- admission information;
- attendance;
- punctuality;
- assessment and attainment;
- educational progress;
- behaviour information;
- SEND information;
- safeguarding information;
- health and medical information;
- dietary information;
- photographs and videos;
- information about educational visits and activities;
- information about use of school systems;
- information required for examinations and assessments; and
- other information needed to support education, welfare and safeguarding.

Parents, carers and legal guardians

- names;
- addresses;
- telephone numbers;
- email addresses;
- relationship to the child;
- information relating to parental responsibility;
- emergency contact information;
- correspondence;
- information relating to court orders or restrictions where relevant;

- payment information where applicable;
- information relating to complaints and concerns; and
- other information needed to communicate with families and support pupils.

Staff and applicants

We may process information including:

- contact details;
- employment history;
- qualifications;
- payroll and pension information;
- attendance and absence;
- appraisal and professional development;
- disciplinary information;
- safeguarding and safer recruitment information;
- DBS and right-to-work information;
- health information where necessary; and
- other information needed to employ and manage staff lawfully.

Governors and volunteers

We may process:

- contact details;
- governance records;
- declarations and interests;
- training records;
- attendance;
- safeguarding information;
- vetting information; and
- information required to enable individuals to carry out their role.

Visitors and contractors

We may process:

- name;
- organisation;
- contact details;
- appointment information;
- visit details;
- identification information;
- vehicle registration details;
- CCTV images;
- safeguarding or access information; and
- other information necessary to manage visits and site security.

5. Special category personal data

Some personal data is particularly sensitive and is subject to additional legal protections.

This includes information about:

- health;
- disability;
- racial or ethnic origin;
- religious or philosophical beliefs;
- genetic data;
- biometric information used for identification;
- sex life; and

- sexual orientation.

The school may need to process special category data in connection with:

- safeguarding;
- SEND;
- medical needs;
- reasonable adjustments;
- religious education and Catholic school provision;
- equality duties;
- staff employment;
- welfare and pastoral support; and
- other statutory responsibilities.

Where we process special category data, we identify an appropriate lawful basis and an additional legal condition for doing so.

6. Criminal offence data

In some circumstances, the school may process information relating to criminal convictions and offences. This may be necessary for purposes such as:

- safeguarding;
- safer recruitment;
- employment;
- risk assessment;
- legal compliance; or
- responding to concerns.

Such information is subject to additional legal requirements and will only be processed where lawful.

7. Where do we get personal information from?

We may collect information directly from the individual concerned.

We may also receive information from:

- parents and carers;
- pupils;
- previous or future schools;
- Peterborough City Council;
- other local authorities;
- the Department for Education;
- health services;
- social care;
- the police;
- safeguarding partners;
- courts and tribunals;
- educational and professional services;
- examination and assessment organisations;
- employers and professional bodies;
- contractors and service providers; and
- other organisations where information sharing is lawful and necessary.

8. Why do we use personal data?

We use personal information to enable us to fulfil our role as a school.

This includes:

Education

We use information to:

- provide teaching and learning;
- assess and monitor progress;
- identify additional needs;
- provide SEND support;
- administer examinations and assessments;
- organise educational visits and activities;
- support attendance;
- report to parents and carers; and
- provide appropriate support and challenge.

Safeguarding and welfare

We use information to:

- protect children and adults from harm;
- respond to safeguarding concerns;
- support pupil welfare;
- manage medical needs;
- work with external agencies;
- respond to emergencies; and
- meet our statutory safeguarding responsibilities.

School administration

We use information to:

- manage admissions;
- maintain school records;
- communicate with families;
- manage attendance;
- organise clubs and activities;
- manage school meals and other services;
- manage payments where applicable;
- manage premises and security;
- maintain school systems; and
- monitor the effective operation of the school.

Employment

We process staff information to:

- recruit and appoint staff safely;
- manage employment;
- pay staff;
- administer pensions and benefits;
- support professional development;
- manage attendance;
- address conduct and performance;
- meet safeguarding responsibilities; and
- comply with employment law.

Governance

We use information to:

- support the work of the Governing Body;
- record governance decisions;
- manage declarations and interests;
- meet statutory governance requirements; and
- demonstrate accountability.

Legal and regulatory responsibilities
We may use information to:

- comply with legal obligations;
- respond to statutory requests;
- fulfil education legislation;
- meet safeguarding requirements;
- cooperate with inspections;
- respond to courts and tribunals;
- investigate incidents; and
- establish, exercise or defend legal claims.

9. Our lawful bases for processing
We will only process personal data where we have a lawful basis under data protection law.
Depending on the circumstances, these may include:
Legal obligation
Where the school is required to process information because the law requires us to do so.
Public task
Where processing is necessary for the performance of a task carried out in the public interest or under official authority.
This is an important lawful basis for much of the school's educational, safeguarding and statutory activity.
Contract
Where processing is necessary to enter into or perform a contract, particularly in relation to employment or services.
Consent
Where we have asked an individual for their permission for a specific use of information.
Consent will only be used where it is an appropriate lawful basis.
Vital interests
Where processing is necessary to protect someone's life in an emergency.
Legitimate interests
Where applicable, the school may process information where it is necessary for a legitimate interest and that processing is permitted by law.
We will not use legitimate interests where another lawful basis is required.

10. Children's information
Children's personal data requires particular care.
Children have their own rights under data protection law.
The school will take account of a child's age, maturity and understanding when considering how information is provided to them and how requests concerning their personal data are handled.
The school will make privacy information available in age-appropriate formats.
Our separate Children's Privacy Notice provides information specifically for pupils.
Current DfE guidance emphasises that children have the same rights over their personal data as adults and that schools should provide privacy information in an age-appropriate way.

11. Parents, carers and children's information

Parents and carers may receive information about their child where this is lawful and appropriate.

Parental responsibility does not automatically give a parent unrestricted access to all information relating to a child.

The school may consider:

- the child's age;
- maturity and understanding;
- the child's wishes;
- confidentiality;
- safeguarding;
- the nature of the information; and
- any relevant legal restrictions.

Our separate Parent/Carer Privacy Notice provides further information.

12. Sharing information

We may share personal information where there is a lawful basis to do so.

This may include sharing with:

- Peterborough City Council;
- other local authorities;
- the Department for Education;
- Ofsted;
- health services;
- NHS services;
- Children's Social Care;
- safeguarding partners;
- the police;
- courts and tribunals;
- examination and assessment organisations;
- professional advisers;
- insurers;
- service providers;
- IT providers;
- catering providers;
- wraparound and activity providers;
- educational professionals; and
- other organisations where the law requires or permits sharing.

We will only share information that is relevant and necessary for the purpose.

We will not routinely share personal information simply because another organisation asks for it.

Where a data processor acts on our behalf, the school will ensure that appropriate contractual and security arrangements are in place.

13. Safeguarding and information sharing

Safeguarding may require information to be shared without an individual's consent.

Where there are reasonable grounds to believe that a child or another person may be at risk of harm, the school may share relevant information with appropriate safeguarding agencies.

Data protection law does not prevent appropriate safeguarding information sharing.

Information will be shared proportionately and through appropriate channels.

14. Department for Education data collections

The school is required to provide certain information to the Department for Education through statutory education data collections.

These may include, where applicable:

- the school census;
- early years collections;
- attendance data;
- assessment and attainment information;
- workforce data;
- pupil characteristic information; and
- other statutory returns.

The information provided through these collections is used for purposes including:

- education funding;
- planning;
- monitoring;
- accountability;
- statistics;
- policy development;
- research; and
- other purposes permitted by law.

The Department for Education may combine information received from schools and other sources.

Where the Department for Education receives personal data and becomes responsible for its own processing, it acts as a separate data controller for that processing.

The DfE publishes its own privacy information concerning how it uses education data, including information held in the National Pupil Database. The current DfE guidance confirms that schools' privacy notices should explain what personal data they share with DfE.

15. National Pupil Database

Some pupil information provided through statutory education collections may contribute to the Department for Education's National Pupil Database (NPD).

The NPD is managed by the Department for Education and contains information from statutory education data collections and other education datasets.

The Department for Education publishes separate information explaining how it processes personal data within the NPD.

The school does not determine how the DfE subsequently uses information once the DfE becomes the relevant data controller.

16. Photographs and videos

The school may take and use photographs and videos for purposes including:

- teaching and learning;
- assessment;
- school records;
- events and performances;
- educational visits;
- sport;
- celebrating pupil achievements;
- school displays;
- newsletters;

- the school website;
- social media;
- publicity; and
- safeguarding.

Identifiable photographs and videos are personal data.
The school will identify an appropriate lawful basis for each use.
Where consent is required or relied upon, the school will record and manage consent appropriately.
Parents, carers, pupils, staff and visitors may have specific restrictions concerning photography or publication, and these will be respected where the school has been informed of them.

17. CCTV and site security

The school may use CCTV to support:

- safeguarding;
- site security;
- crime prevention and investigation;
- protection of pupils, staff and visitors;
- investigation of incidents; and
- protection of school property.

CCTV footage will only be accessed by authorised individuals.
Footage will be retained for an appropriate period and may be retained for longer where it is required for an investigation, safeguarding matter, complaint or legal proceedings.

18. Filtering and monitoring

The school uses filtering and monitoring systems as part of its safeguarding and online safety arrangements.
Depending on the systems used, monitoring may include information such as:

- websites visited;
- searches;
- online activity;
- files or content;
- communication activity;
- system alerts; and
- information identified by filtering or monitoring tools.

The purpose is to:

- protect children from harmful or illegal content;
- identify safeguarding concerns;
- support online safety;
- protect school systems; and
- meet our safeguarding responsibilities.

Monitoring information is accessible only to authorised staff and relevant technical service providers.
Where monitoring identifies a safeguarding concern, relevant information may be transferred to safeguarding records.

19. Artificial intelligence and digital technology

The school may use approved digital services, including AI-enabled technologies, where these support teaching, learning, safeguarding or school administration.
Before introducing a system which processes personal data, the school will consider:

- the purpose of processing;
- lawful basis;
- security;

- retention;
- data sharing;
- international transfers;
- provider arrangements;
- risks to children and other individuals; and
- whether a Data Protection Impact Assessment is required.

Staff must not enter confidential or unnecessary personal information into an AI tool unless its use has been authorised and is lawful.
Where AI or automated tools are used, the school will not assume that outputs are accurate simply because they are generated by technology.
The school will not normally make decisions about individuals based solely on automated processing where that would have legal or similarly significant effects without meeting the applicable legal requirements.

20. Educational technology
The school uses a range of digital and cloud-based systems to support education and administration.
These may include:

- management information systems;
- safeguarding systems;
- assessment systems;
- communication platforms;
- learning platforms;
- finance and payment systems;
- catering systems;
- online safety systems;
- visitor-management systems; and
- other educational technology.

Before using a new system, the school will consider its data protection and security implications.
Where a third party processes personal data for the school, appropriate contractual arrangements will be put in place.
The school will seek to ensure that personal data collected through educational technology is necessary, proportionate and secure.
The ICO's current work on educational technology reinforces the importance of responsible and transparent processing of children's information by edtech providers.

21. International transfers
Some of the organisations that provide services to schools may process information outside the United Kingdom.
Where personal data is transferred outside the UK, the school will ensure that the transfer complies with applicable data protection law and that appropriate safeguards are in place.
The school will consider international transfers when procuring and reviewing relevant services.

22. How we keep information secure
We use appropriate technical and organisational measures to protect personal information.
These may include:

- access controls;
- passwords and authentication;
- secure networks;
- encryption where appropriate;
- filtering and monitoring;

- secure cloud systems;
- staff training;
- locked storage;
- secure disposal;
- confidentiality arrangements;
- backups; and
- physical security.

Access to personal information is limited to those who need it for legitimate school purposes.

23. Personal data breaches

A personal data breach includes:

- accidental disclosure;
- loss of information;
- theft of a device;
- unauthorised access;
- sending information to the wrong person;
- accidental publication; or
- another security incident affecting personal data.

All suspected breaches must be reported to the school immediately.

The school will investigate breaches and determine whether further action is required, including notification to the Information Commissioner's Office or affected individuals where legally required.

The school will keep an appropriate record of personal data breaches and decisions concerning them.

24. How long we keep personal information

The school will not retain personal data for longer than necessary.

Different categories of information have different retention periods.

The school's Data Retention Policy and Data Retention Schedule set out the school's retention arrangements.

Information may be retained for longer where this is necessary because of:

- safeguarding;
- legal proceedings;
- complaints or investigations;
- financial or audit requirements;
- statutory obligations;
- employment requirements; or
- another legitimate reason.

When information is no longer required, it will be securely deleted, destroyed or anonymised.

25. Your data protection rights

Depending on the circumstances, individuals may have rights to:

- be informed about how their information is used;
- request access to their personal data;
- have inaccurate information corrected;
- request erasure of information;
- request restriction of processing;
- object to certain processing;
- request data portability; and
- have rights relating to certain automated decision-making and profiling.

These rights are subject to legal conditions and exemptions.

The school will respond to requests in accordance with current data protection legislation.

26. Subject Access Requests
You have the right to request access to personal data the school holds about you.
A Subject Access Request may be made verbally or in writing.
Requests should be sent to the school or Data Protection Officer.
The school will normally respond within one calendar month, subject to the applicable legal provisions.
Where a request is complex or an individual has made multiple requests, the law may allow additional time.

27. Rectification
You can ask the school to correct personal information that you believe is inaccurate or incomplete.
The school will consider the request and update information where appropriate.
Where information cannot be changed immediately, the school may record the fact that its accuracy is disputed while the matter is considered.

28. Erasure
In some circumstances, individuals can request that personal information is deleted.
However, this right does not apply in every situation.
For example, the school may need to retain information because:

- the law requires it;
- it is necessary for safeguarding;
- it is needed for the exercise of official authority;
- there is an ongoing legal matter; or
- another legal exemption applies.

29. Restriction and objection
In certain circumstances, individuals may ask the school to restrict processing or object to particular processing.
The school will consider requests in accordance with the applicable legal requirements.

30. Children's rights
Children have their own data protection rights.
The school will take account of a child's age, maturity and understanding when dealing with requests.
A parent or carer may sometimes make a request on behalf of a child, but parental responsibility does not automatically give access to all of a child's personal information.
The school will consider the child's rights, wishes, confidentiality and welfare.

31. Data portability
The right to data portability applies only in certain circumstances, particularly where personal data is processed:

- by automated means;
- on the basis of consent or contract; and
- in a way covered by the applicable legal requirements.

Where the right applies, the school will comply with the legal requirements.

32. Automated decision-making

The school does not routinely make decisions about pupils, parents, staff or visitors based solely on automated processing where such decisions produce legal or similarly significant effects.

Where this changes, the school will ensure that the applicable legal requirements are considered and that individuals receive appropriate information.

33. Data processors

The school uses external organisations to provide some services.

Examples may include:

- IT support;
- cloud services;
- school management systems;
- safeguarding platforms;
- catering systems;
- payment systems;
- online learning platforms;
- communication systems;
- visitor management;
- professional services; and
- other specialist providers.

Where a supplier processes personal data on behalf of the school, appropriate contractual requirements will apply.

The school will take reasonable steps to ensure that processors:

- process information only for authorised purposes;
- maintain confidentiality;
- maintain appropriate security;
- notify the school of relevant breaches;
- support the exercise of data protection rights; and
- securely delete or return information when required.

34. Records of Processing Activities

The school maintains appropriate records of its processing activities.

These records help the school understand:

- what personal data it processes;
- why it is processed;
- the lawful basis;
- who receives the information;
- how information is protected;
- how long it is retained; and
- where relevant, whether information is transferred internationally.

Records are reviewed when significant processing changes occur.

35. Data Protection Impact Assessments

The school will complete a Data Protection Impact Assessment (DPIA) where required.

A DPIA may be relevant when introducing:

- new technology;
- CCTV;
- significant monitoring systems;
- biometric technology;

- AI systems;
- large-scale processing of special category data;
- significant data-sharing arrangements; or
- other processing likely to result in a high risk to individuals.

The DPO will advise on DPIAs and related privacy risks.

36. Changes to this Privacy Notice

We may update this Privacy Notice from time to time to reflect:

- changes in law;
- changes in DfE or ICO guidance;
- changes to school systems;
- new services;
- changes to the way personal data is processed; or
- improvements to transparency.

The current version will be made available through the school website.
The DPO will review the notice at least annually and whenever there is a significant change to processing.

37. Complaints

The school takes concerns about personal data seriously.
We encourage individuals to contact the school or DPO first so that we can investigate and resolve the issue where possible.
School
St John Henry Newman Catholic Primary School
Aqua Drive
Hampton Water
Peterborough
PE7 8QL
Telephone: 01733 304533
Email: office@stjhn.org.uk
Data Protection Officer
The ICT Service
Email: dpo@theictservice.org.uk
Telephone: 0300 300 0000, option 1
Individuals also have the right to complain directly to the Information Commissioner's Office (ICO).
ICO helpline: 0303 123 1113

38. Information Commissioner's Office

The ICO is the independent regulator for data protection in the UK.
The ICO provides guidance on data protection rights and investigates concerns about the handling of personal information.
The school will cooperate with the ICO where required.

39. Further information

This Privacy Notice should be read alongside the school's:

- Data Protection Policy;
- Data Retention Policy;
- Data Retention Schedule;
- Parent/Carer Privacy Notice;
- Children's Privacy Notice;

- Visitor Privacy Notice;
- Staff privacy information;
- Safeguarding and Child Protection Policy;
- Online Safety Policy;
- Acceptable Use arrangements;
- CCTV arrangements; and
- other relevant information governance documents.

Appendix 1 – Privacy Information for Different Groups

The school provides additional audience-specific privacy information to make information easier to understand.

Parents and carers

Our Parent/Carer Privacy Notice explains how we process information about parents, carers and legal guardians.

Children

Our Children's Privacy Notice explains data protection in an age-appropriate format for pupils.

Visitors

Our Visitor Privacy Notice explains how information about visitors and contractors is processed.

Staff

Staff receive separate privacy information explaining how their personal information is processed in connection with employment and recruitment.

Governors

Governors receive appropriate information concerning the processing of personal data in connection with their governance role.

All of these notices should be read alongside this overarching Privacy Notice.

Appendix 2 – Our Privacy Principles

At St John Henry Newman Catholic Primary School, we aim to ensure that personal data is:

Lawful

We only use information where there is a lawful reason.

Fair

We use information in a way people would reasonably expect.

Transparent

We explain what we do with information.

Necessary

We do not collect or retain information without a legitimate purpose.

Accurate

We seek to keep information correct and up to date.

Secure

We take appropriate steps to protect information.

Accountable

We maintain appropriate records and can demonstrate how we comply with data protection requirements.

These principles reflect the data protection framework applying to schools in England.