St John Henry Newman

Catholic Primary School

Data Protection Policy

Approved: September 2026

Next Review Date: September 2028

1. Introduction

St John Henry Newman Catholic Primary School is committed to protecting the privacy and security of personal data relating to pupils, parents and carers, staff, governors, volunteers, visitors, contractors and other individuals.

The school recognises that the lawful and secure handling of personal data is an essential part of its responsibilities as a school and as a Catholic community. Personal data must be processed fairly, lawfully, transparently and securely, and only where there is a clear and legitimate purpose for doing so.

This policy applies to all personal data processed by or on behalf of the school, whether held electronically, on paper or in any other form.

It applies to all governors, employees, supply staff, volunteers, contractors, visitors and other individuals who process personal data on behalf of the school.

Failure to comply with this policy may result in disciplinary action and, where appropriate, referral to external agencies or regulatory bodies.

2. Legal framework

This policy is based on the following legislation and guidance:

- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025;
- Privacy and Electronic Communications Regulations 2003 (PECR), where applicable;
- Protection of Freedoms Act 2012, where biometric information is processed;
- Freedom of Information Act 2000, where applicable;
- Education (Pupil Information) (England) Regulations 2005, where applicable;
- Keeping Children Safe in Education;
- Department for Education guidance on data protection in schools;
- Department for Education guidance on filtering and monitoring;
- Information Commissioner's Office (ICO) guidance and codes of practice; and
- other relevant statutory guidance and legislation.

The Data (Use and Access) Act 2025 introduced changes to UK data protection law which are now in force. This policy therefore reflects the current legal framework as at September 2026.

The school will review this policy and associated procedures when legislation, statutory guidance or ICO requirements change.

3. Data protection principles

The school will comply with the data protection principles. Personal data must be:

1. **Processed lawfully, fairly and transparently.**
2. **Collected for specified, explicit and legitimate purposes** and not processed in a manner incompatible with those purposes.
3. **Adequate, relevant and limited to what is necessary** for the purposes for which it is processed.
4. **Accurate and, where necessary, kept up to date.**
5. **Kept for no longer than is necessary** for the purposes for which it is processed.
6. **Processed securely**, using appropriate technical and organisational measures.

The school will also comply with the principle of **accountability**, meaning that it must be able to demonstrate compliance with data protection law.

4. Definitions

Personal data

Personal data means information relating to an identified or identifiable living individual.

This may include:

- names and addresses;
- contact details;
- dates of birth;
- pupil and staff identification numbers;
- photographs and videos;
- CCTV images;
- online identifiers;
- IP addresses and device information;
- attendance, behaviour and attainment information;
- safeguarding information;
- medical information;
- financial information;
- employment information; and
- information contained within school communications and records.

Special category data

Special category data is personal data requiring additional protection because of its sensitivity. This includes information relating to:

- racial or ethnic origin;
- religious or philosophical beliefs;
- health;
- trade union membership;
- genetic data;
- biometric data used for identification;
- sex life; and
- sexual orientation.

Criminal offence data

Information relating to criminal convictions and offences, or related security measures, is subject to additional legal requirements.

Processing

Processing means anything done with personal data, including collecting, recording, storing, organising, accessing, using, sharing, altering, transferring, restricting, deleting or destroying it.

Data controller

The school is the data controller for personal data for which it determines the purposes and means of processing.

Data processor

A data processor is an organisation or individual that processes personal data on behalf of the school.

Data subject

A data subject is an identified or identifiable individual whose personal data is being processed.

Personal data breach

A personal data breach is a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

5. Data controller and governance

St John Henry Newman Catholic Primary School is the data controller for the personal data it processes.

The **Governing Body** has overall accountability for ensuring that the school complies with data protection law.

Governors will:

- ensure that appropriate data protection arrangements are in place;

- receive appropriate assurance regarding compliance;
- ensure that the school has suitable policies and procedures;
- support appropriate data protection training;
- ensure that appropriate resources are available;
- oversee significant data protection risks; and
- receive information about significant breaches and compliance issues.

The Department for Education confirms that governing bodies are responsible for ensuring that schools comply with data protection requirements and that appropriate governance arrangements are in place.

6. Data Protection Officer

The school will appoint a Data Protection Officer (DPO) in accordance with the UK GDPR.

The DPO will:

- advise the school, governors and staff on data protection obligations;
- monitor compliance with data protection legislation and this policy;
- provide advice on Data Protection Impact Assessments (DPIAs);
- advise on data protection risks;
- support staff training and awareness;
- maintain appropriate records;
- act as a contact point for individuals and the ICO;
- advise on personal data breaches;
- support the development and review of privacy notices; and
- provide appropriate reports and assurance to the Governing Body.

The DPO must be sufficiently independent, appropriately qualified and adequately resourced to perform their role.

The school will publish appropriate DPO contact information through its privacy notices.

7. Responsibilities

7.1 Headteacher

The Headteacher is responsible for the day-to-day implementation of this policy and ensuring that appropriate arrangements are in place across the school.

The Headteacher will work with the DPO and relevant staff to ensure that data protection is incorporated into school procedures and decision-making.

7.2 Senior leaders

Senior leaders are responsible for:

- ensuring staff understand their data protection responsibilities;
- ensuring appropriate security arrangements are maintained;
- considering data protection when introducing new systems or processes;
- ensuring data sharing is lawful and proportionate;
- ensuring staff report breaches promptly; and
- supporting monitoring and compliance.

7.3 All staff, governors and volunteers

Everyone who handles personal data on behalf of the school is responsible for:

- following this policy and associated procedures;
- only accessing information they need for their role;
- keeping personal data secure;
- not sharing personal data without appropriate authority;
- reporting suspected breaches immediately;
- ensuring paper and electronic records are handled securely;
- following retention and disposal requirements; and
- seeking advice where they are unsure.

Staff must not assume that information can be shared simply because they have access to it.

8. Lawful processing

The school will only process personal data where there is a lawful basis under the UK GDPR.

Depending on the circumstances, these may include:

- consent;
- performance of a contract;
- compliance with a legal obligation;
- protection of vital interests;
- performance of a task carried out in the public interest or in the exercise of official authority; and
- legitimate interests, where applicable.

For special category data, the school will also identify an appropriate additional condition for processing.

For criminal offence data, the school will identify both an appropriate lawful basis and an applicable condition under data protection law.

The school will not rely on consent where another lawful basis is more appropriate.

Where consent is used, it must be freely given, specific, informed and capable of being withdrawn. The school will maintain appropriate records of consent.

The ICO confirms that public task is particularly relevant to schools when processing is necessary to perform a specific task in the public interest or under official authority.

9. Transparency and privacy notices

The school will provide clear and accessible privacy information to individuals about how their personal data is collected and used.

Privacy notices will explain, as appropriate:

- what personal data is collected;
- why it is collected;
- the lawful basis for processing;
- how the information is used;
- who it may be shared with;
- how long it is retained;
- individuals' rights;
- how individuals can raise concerns;
- the role and contact details of the DPO;
- the school's use of photographs and videos;
- CCTV arrangements;
- filtering and monitoring;
- relevant use of educational technology and AI; and
- how to contact the ICO.

Privacy notices will be reviewed at least annually and whenever there is a significant change in the school's processing activities. DfE guidance states that schools must make privacy notices freely available and keep them under review.

10. Data minimisation and accuracy

The school will only collect personal data that is adequate, relevant and necessary for the intended purpose.

Staff must not collect additional personal information simply because it may be useful in the future.

The school will take reasonable steps to ensure personal data is:

- accurate;
- complete where necessary;
- up to date; and
- corrected or deleted when inaccurate and no longer required.

Staff should report inaccurate information to the appropriate member of staff as soon as possible.

11. Records of Processing Activities

The school will maintain an appropriate **Record of Processing Activities (ROPA)**.

This will identify, as appropriate:

- the categories of personal data processed;
- the categories of data subjects;
- purposes of processing;
- lawful bases;
- special category conditions;
- recipients of information;
- international transfers;
- retention periods;
- security measures;
- data processors; and
- relevant data sharing arrangements.

The ROPA will be reviewed regularly and updated when processing activities change.

DfE guidance identifies the ROPA as an important means of demonstrating accountability and recommends recording the school's personal data assets, purposes, recipients, retention and security arrangements.

12. Data protection by design and default

Data protection will be considered when:

- introducing new technology;
- purchasing new software or systems;
- changing administrative processes;
- collecting new categories of personal data;

- introducing monitoring systems;
- introducing AI-enabled technology;
- changing data-sharing arrangements; or
- undertaking projects involving significant amounts of personal data.

The school will consider privacy and security from the beginning of a project rather than as an afterthought.

---

13. Data Protection Impact Assessments

The school will complete a **Data Protection Impact Assessment (DPIA)** where processing is likely to result in a high risk to individuals' rights and freedoms.

A DPIA will also be considered before introducing:

- new technologies;
- CCTV systems or significant changes to them;
- filtering and monitoring systems;
- biometric systems;
- AI systems;
- systems involving large amounts of special category data;
- significant data-sharing arrangements; or
- other processing presenting significant privacy risks.

The DPO will advise on whether a DPIA is required and on appropriate mitigations.

DPIAs will be reviewed where processing changes or new risks emerge.

14. Data sharing

Personal data will only be shared where there is a lawful basis and the sharing is necessary, proportionate and fair.

The school may share information with, for example:

- the Department for Education;
- Peterborough City Council;
- other local authorities;
- health services;
- social care;
- the police;
- safeguarding partners;

- courts and tribunals;
- examination and assessment organisations;
- professional advisers;
- contracted service providers; and
- other organisations where legally required or permitted.

Consent will not necessarily be required where information must or may lawfully be shared without consent, including safeguarding circumstances.

Safeguarding concerns must never be delayed because of uncertainty about data protection. Staff should seek advice from the DSL and/or DPO where necessary.

Where data is shared with a processor, the school will ensure that appropriate contractual arrangements and safeguards are in place.

The school will share the minimum information necessary for the purpose.

15. International transfers

Where personal data is transferred outside the UK, the school will ensure that the transfer complies with applicable UK data protection law and that appropriate safeguards are in place.

Staff must seek advice from the DPO before arranging a new international transfer of personal data.

16. Subject Access Requests

Individuals have the right to request access to their personal data.

A Subject Access Request (SAR) can be made verbally or in writing and does not have to use a particular form.

Any member of staff receiving a SAR must immediately refer it to the appropriate member of staff/DPO.

The school will:

- acknowledge the request where appropriate;
- establish the identity of the requester where reasonably necessary;
- clarify the request where clarification is reasonably required;
- conduct a reasonable and proportionate search;
- consider relevant exemptions and restrictions;
- provide information securely; and
- respond without undue delay and normally within one calendar month.

The response period may be extended by up to a further two months where the request is complex or where an individual has made a number of requests.

The school may charge a reasonable fee where permitted by law, including for manifestly unfounded or excessive requests or additional copies.

Current ICO guidance confirms that SARs should normally be answered within one month, with a possible extension of up to two additional months for complex or multiple requests.

17. Children's data and parental requests

Children have their own data protection rights.

The school will consider a child's age, maturity and understanding when deciding whether they are able to exercise their rights themselves.

A parent or carer may make a request on behalf of a child in appropriate circumstances, but parental responsibility does not automatically entitle a parent to all information relating to a child.

The school will consider:

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

The school will comply with the separate statutory requirements relating to access to educational records where applicable.

18. Other individual rights

Depending on the circumstances, individuals may have rights to:

- be informed;
- access their personal data;
- rectify inaccurate data;
- request erasure;
- restrict processing;
- object to processing;
- data portability; and
- rights relating to automated decision-making and profiling.

These rights are not absolute and may be subject to legal exemptions or restrictions.

All requests should be referred promptly to the DPO.

19. Photographs and videos

Photographs and videos of identifiable individuals are personal data and must be processed in accordance with data protection law.

The school may use photographs and videos for purposes including:

- teaching and learning;
- assessment;
- safeguarding;
- school administration;
- displays;
- school newsletters;
- the school website;
- social media;
- publicity;
- performances;
- sporting events;
- educational visits; and
- other legitimate school activities.

The school will identify an appropriate lawful basis for each use.

Where consent is relied upon, the school will maintain appropriate records and respect withdrawals of consent.

Staff must:

- use school-approved equipment and systems wherever possible;
- avoid storing school photographs on personal devices;
- transfer images securely to school systems;
- delete images from temporary storage when no longer required; and
- check relevant restrictions before publishing images.

The school will take particular care where pupils have safeguarding concerns, court orders or other restrictions preventing publication.

Current DfE guidance confirms that identifiable photographs and videos are personal data and should be stored, shared and disposed of securely.

20. CCTV

Where the school operates CCTV, it will be used only for defined and proportionate purposes such as:

- safeguarding;
- site security;
- preventing and investigating crime;
- protecting pupils, staff and visitors;
- supporting emergency response; and
- protecting school property.

The school will:

- display appropriate CCTV signage;
- explain CCTV use through its privacy information;
- restrict access to authorised staff;
- maintain appropriate security;
- retain footage only for as long as necessary;
- respond appropriately to requests for footage;
- maintain appropriate records; and
- review the system and its operation regularly.

The school will not normally use facial recognition or audio recording through CCTV. Any proposal to introduce such functionality would require careful consideration, appropriate authorisation and a DPIA.

DfE guidance identifies CCTV as personal-data processing and recommends proportionate use, clear signage, restricted access, appropriate retention and DPIA consideration.

21. Filtering and monitoring

The school recognises that filtering and monitoring form part of its safeguarding and online safety arrangements.

Filtering is preventative and seeks to prevent access to illegal, inappropriate or harmful online content.

Monitoring is reactive and may identify or record potentially harmful or inappropriate activity.

The school will:

- maintain appropriate filtering and monitoring arrangements;
- ensure monitoring data is accessible only to authorised individuals;
- ensure staff with access receive appropriate training;
- maintain clear procedures for responding to alerts;

- retain monitoring information only for an appropriate period;
- ensure filtering and monitoring arrangements are reflected in privacy information;
- review the effectiveness of arrangements regularly; and
- complete a DPIA before introducing a new system or making significant changes.

Where third-party providers operate filtering or monitoring systems, the school will ensure that appropriate contractual and data protection arrangements are in place.

DfE guidance specifically requires schools to consider the data protection implications of filtering and monitoring, including access, retention, privacy notices and DPIAs.

22. Artificial Intelligence

The school recognises that AI tools may involve the processing of personal data.

Staff must not enter confidential or personal information about pupils, parents, staff or other individuals into an AI system unless:

- the use has been authorised;
- an appropriate lawful basis exists;
- the system has been appropriately assessed;
- the school's data protection and security requirements are satisfied; and
- the DPO or relevant senior leader has confirmed that the proposed use is appropriate where required.

Staff must consider whether personal data is genuinely necessary before using an AI tool.

The school will consider:

- what data is entered;
- where the data is processed;
- whether data is retained by the provider;
- whether data is used to train the provider's model;
- who can access the information;
- whether information is transferred outside the UK;
- accuracy and bias;
- safeguarding implications; and
- whether a DPIA is required.

AI outputs must not be treated as automatically accurate or appropriate.

DfE guidance specifically highlights the data protection risks associated with generative AI and recommends careful consideration of children's privacy when using AI.

23. Educational technology and third-party providers

Before procuring or introducing a new digital system that processes personal data, the school will consider:

- the purpose of processing;
- the lawful basis;
- what information is collected;
- whether the processing is necessary and proportionate;
- the provider's data protection arrangements;
- security arrangements;
- retention;
- data sharing;
- international transfers;
- deletion arrangements;
- sub-processors;
- parental and pupil transparency;
- accessibility; and
- whether a DPIA is required.

The school will not introduce technology solely because it is available. The educational or operational benefit must justify the processing of personal data.

24. Data security

The school will implement appropriate technical and organisational measures to protect personal data.

These may include:

- password protection;
- appropriate access controls;
- role-based permissions;
- secure networks;
- encryption where appropriate;
- secure cloud services;
- antivirus and security software;
- filtering and monitoring;
- secure backups;
- locked storage;

- confidential waste arrangements;
- secure disposal;
- staff training; and
- physical security.

Staff must:

- keep passwords confidential;
- lock or secure devices when unattended;
- avoid leaving confidential information visible;
- collect documents promptly from printers;
- use approved school systems;
- avoid using personal email accounts for school business;
- avoid storing school data on personal devices unless explicitly authorised;
- check recipients carefully before sending information; and
- report mistakes immediately.

25. Working away from school

Staff should only take personal data away from school where this is necessary and proportionate.

Particular care must be taken with:

- safeguarding records;
- medical information;
- SEND information;
- personnel records;
- confidential correspondence; and
- other special category data.

Where personal data is taken away from school, staff must use appropriate security measures and ensure that information cannot be accessed by unauthorised individuals.

26. Data retention and disposal

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

Retention periods will be determined by:

- statutory requirements;
- regulatory requirements;
- the purpose for which information is processed;

- legal claims or disputes;
- safeguarding requirements;
- financial and audit requirements; and
- relevant records management guidance.

The school will maintain a separate **Data Retention Schedule**.

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

Confidential paper records must be disposed of using an appropriate confidential waste process.

Electronic information must be securely deleted where appropriate.

27. Personal data breaches

All suspected or actual personal data breaches must be reported **immediately** to the DPO or designated school data protection contact.

Examples include:

- sending information to the wrong person;
- losing a laptop or USB device;
- losing a paper file;
- accidental disclosure;
- unauthorised access;
- inappropriate sharing;
- phishing or cyberattack;
- publishing information accidentally;
- leaving confidential information unsecured;
- sending an email to the wrong recipient; or
- loss or theft of a device containing personal data.

Staff must not delay reporting a breach because they believe it is minor or because they are concerned about potential consequences.

The DPO will:

1. establish what happened;
2. contain the breach;
3. assess the risks;
4. identify affected individuals;

5. determine whether notification to the ICO is required;
6. determine whether affected individuals need to be informed;
7. record the decision and actions taken;
8. implement remedial measures; and
9. consider whether further training or changes to procedures are required.

Where a breach is notifiable to the ICO, the school will normally notify the ICO within **72 hours of becoming aware of it**, unless the legislation provides otherwise.

All breaches, including those which are not externally reportable, will be recorded appropriately.

28. Reporting breaches

Any person who identifies a potential breach must report it immediately.

The school will operate a culture in which staff are encouraged to report mistakes promptly. Early reporting allows the school to reduce potential harm.

A breach report will not automatically result in disciplinary action. The school will consider the circumstances, including whether the individual acted honestly, followed procedures and reported the incident promptly.

Intentional, reckless or repeated breaches may be addressed through the school's disciplinary procedures.

29. Data processors

Where an external organisation processes personal data on behalf of the school, the school will ensure appropriate contractual arrangements are in place.

Contracts will address, as appropriate:

- the purpose and duration of processing;
- the categories of personal data;
- the categories of data subjects;
- security requirements;
- confidentiality;
- sub-processors;
- data breach reporting;
- data subject rights;
- deletion or return of data;
- audits and compliance;
- international transfers; and

- appropriate assistance to the school.

The school will undertake appropriate due diligence before appointing significant data processors.

30. Confidentiality

Personal data must only be accessed by individuals who require it for legitimate school purposes.

Staff must not discuss confidential information:

- in public areas;
- with individuals who are not authorised to receive it;
- through personal social media;
- through personal email accounts; or
- through other unauthorised communication channels.

Particular care must be taken with safeguarding, SEND, medical, disciplinary and personnel information.

31. Governors

Governors may have access to personal data where this is necessary for the proper discharge of their governance responsibilities.

Governors must:

- only access information necessary for their role;
- maintain confidentiality;
- comply with this policy;
- use approved systems;
- securely dispose of information;
- not share confidential information outside authorised channels; and
- refer data protection concerns to the Headteacher or DPO.

Where governors receive confidential papers, these must be stored securely and disposed of appropriately.

32. Training

All staff will receive appropriate data protection training.

Training will cover, as appropriate:

- data protection principles;
- confidentiality;

- secure handling of information;
- passwords and cyber security;
- phishing;
- data breaches;
- subject access requests;
- safeguarding information;
- photographs and videos;
- AI;
- filtering and monitoring;
- data sharing; and
- the school's reporting arrangements.

New staff will receive appropriate data protection information as part of induction.

Training will be refreshed periodically and when significant changes occur.

33. Complaints

Individuals who have concerns about the school's handling of their personal data should initially contact the school or DPO.

The school will investigate complaints and take appropriate action.

Individuals also have the right to complain directly to the Information Commissioner's Office.

Information about how to contact the ICO will be included in the school's privacy information.

34. Monitoring and compliance

The school will monitor compliance through:

- review of data protection arrangements;
- audits;
- review of the ROPA;
- DPIA reviews;
- data breach monitoring;
- staff training records;
- review of data processors;
- review of privacy notices;

- review of retention arrangements;
- review of filtering and monitoring;
- review of CCTV arrangements;
- governor oversight; and
- advice and assurance from the DPO.

The school will take appropriate action where weaknesses are identified.

35. Related policies and documents

This policy should be read alongside:

- Privacy Notices;
- Data Retention Schedule;
- Data Breach Procedure;
- Subject Access Request Procedure;
- Freedom of Information Policy;
- Information Security / Cyber Security arrangements;
- Acceptable Use Policy;
- Online Safety Policy;
- Safeguarding and Child Protection Policy;
- Staff Code of Conduct;
- CCTV Policy, where applicable;
- Photography and Video Policy, where applicable;
- Records Management arrangements;
- AI guidance;
- Filtering and Monitoring arrangements; and
- relevant contracts and data processing agreements.

Appendix 1 – Personal Data Breach Procedure

Step 1 – Report immediately

Report the breach or suspected breach to the DPO or designated school data protection contact.

Step 2 – Contain the breach

Take immediate reasonable steps to prevent further disclosure or loss.

For example:

- recall an email where possible;
- contact the recipient and request deletion;
- secure a misplaced document;
- disable a compromised account;
- change a compromised password; or
- contact the IT provider where necessary.

Step 3 – Assess

The DPO will consider:

- what information was involved;
- whose information was affected;
- how many individuals were affected;
- whether special category or safeguarding information was involved;
- who received or accessed the information;
- whether the information was encrypted;
- the likelihood of harm; and
- the potential severity of harm.

Step 4 – Record

The school will maintain an appropriate breach record, including breaches that do not require notification to the ICO.

Step 5 – Notify

Where required, the school will notify:

- the ICO;
- affected individuals;
- the police;
- safeguarding partners; or

- other relevant organisations.

Step 6 – Learn

Following significant breaches, the school will review:

- what happened;
- why it happened;
- whether procedures were followed;
- whether additional training is required; and
- whether systems or procedures should be changed.

Appendix 2 – Staff Data Protection: Quick Reference

Staff should remember:

STOP

Stop before sharing personal data.

CHECK

Check that you have a lawful reason and that the recipient is authorised.

MINIMISE

Only share the information that is necessary.

SECURE

Use approved school systems and keep information secure.

REPORT

Report mistakes and suspected breaches immediately.

ASK

If you are unsure, ask the DPO or appropriate senior leader before processing or sharing the information.

A data protection mistake that is reported immediately can often be contained. A mistake that is hidden can become a much more serious issue.

Appendix 3 – Key Data Protection Contacts

Data Controller:
St John Henry Newman Catholic Primary School

Headteacher:
Headteacher, St John Henry Newman Catholic Primary School

Data Protection Officer:
The school's appointed Data Protection Officer. Current contact details are published in the school's privacy notices.

School contact:
office@st-johnhenrynewman.org.uk

Regulator:
Information Commissioner's Office (ICO)

The school's current privacy notices should always be used for the most up-to-date contact details.