St John Henry Newman

Catholic Primary School

Data Retention Policy

Approved: September 2026

Next Review Date: September 2028

1. Purpose

St John Henry Newman Catholic Primary School is committed to managing information responsibly throughout its lifecycle.

The school recognises that personal data must not be retained indefinitely simply because it may be useful in the future. Information should be retained only for as long as there is a legitimate, legal or operational reason to do so and should then be securely destroyed, deleted or anonymised.

This policy supports the school's **Data Protection Policy** and provides the framework for determining:

- what information the school retains;
- why it is retained;
- how long it is retained;
- where it is stored;
- who has access to it; and
- how it is securely disposed of.

The policy applies to information held electronically, on paper and in any other format.

2. Legal framework

This policy operates within the requirements of:

- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025;
- Freedom of Information Act 2000, where applicable;
- Education (Pupil Information) (England) Regulations 2005;
- Keeping Children Safe in Education;
- Department for Education records management and data protection guidance;
- Information Commissioner's Office guidance; and
- other relevant statutory and regulatory requirements.

The UK GDPR requires personal data to be kept for no longer than is necessary for the purposes for which it is processed.

The school will therefore apply appropriate retention periods rather than retaining personal data indefinitely.

3. Scope

This policy applies to information relating to:

- pupils and former pupils;
- parents and carers;
- staff and former staff;
- governors;
- volunteers;
- applicants;
- visitors;
- contractors;
- suppliers; and
- other individuals whose personal data is processed by the school.

It applies to:

- electronic records;
- paper records;
- emails;
- databases;
- photographs and videos;
- CCTV;
- safeguarding records;
- online systems;
- cloud storage;
- staff records;
- financial records;
- educational records; and
- information held by third-party processors on behalf of the school.

4. Principles

The school will apply the following principles to retention.

4.1 Necessity

Information will only be retained where there is a continuing legitimate, legal or operational reason.

4.2 Proportionality

The school will retain only the information necessary for the relevant purpose.

4.3 Accuracy

Records retained for an extended period will be reviewed and corrected where necessary.

4.4 Security

Information will remain appropriately protected throughout its retention period.

4.5 Accountability

The school will maintain a **Data Retention Schedule** setting out agreed retention periods for significant categories of information.

4.6 Secure disposal

When the retention period expires, information will be securely destroyed, deleted or anonymised unless there is a legitimate reason for further retention.

5. Data Retention Schedule

The school's detailed **Data Retention Schedule** forms part of this policy.

The schedule will identify, where appropriate:

- record category;
- examples of information covered;
- retention period;
- start point for the retention period;
- storage location;
- responsible owner;
- disposal method; and
- any relevant statutory or regulatory basis.

The schedule will be reviewed at least annually and whenever legislation or relevant guidance changes.

Where a statutory retention period applies, the school will comply with that requirement.

Where no statutory period applies, the school will determine a proportionate retention period based on:

- the purpose for processing;
- legal requirements;
- safeguarding considerations;
- potential legal claims;
- financial and audit requirements;
- educational requirements;
- operational need;
- the sensitivity of the information; and
- the potential impact on individuals if information were retained unnecessarily.

6. Retention periods

Retention periods will normally begin from an appropriate **trigger date**, rather than necessarily from the date the information was created.

Examples include:

- the pupil leaving the school;
- the employee leaving employment;
- the conclusion of a safeguarding matter;
- the completion of an investigation;
- the end of a financial year;
- the completion of a contract;
- the conclusion of a complaint; or
- the date of the last relevant activity.

The school's Data Retention Schedule will specify the appropriate trigger date for each category.

7. Safeguarding and child protection records

Safeguarding and child protection records require particular care.

The school will retain safeguarding records in accordance with current statutory guidance and relevant records management requirements.

Safeguarding records must:

- be stored securely;
- have access restricted to appropriate staff;
- be retained separately or appropriately flagged within safeguarding systems;
- not be routinely deleted when a pupil changes class or staff member;
- be transferred securely when a pupil moves school where appropriate; and
- be disposed of securely when the relevant retention period expires.

Where there is uncertainty about whether a safeguarding record should be destroyed, the DSL will seek advice from the DPO and, where necessary, the local authority safeguarding team or other appropriate professional body.

Safeguarding considerations may justify retention beyond an ordinary administrative retention period.

8. Educational and pupil records

Pupil records will be retained in accordance with applicable education legislation and records management guidance.

The school will distinguish between:

- the pupil's educational record;
- routine teaching and learning information;
- assessment information;
- attendance records;
- behaviour records;
- SEND information;
- safeguarding records; and
- administrative information.

Not all information relating to a pupil requires the same retention period.

Working notes, duplicate documents and temporary information should not automatically be retained as part of the permanent pupil record.

9. SEND and medical information

Information relating to SEND and medical needs may include special category personal data and must be handled with particular care.

The school will retain information where it is necessary to:

- support the pupil's education;
- meet statutory duties;
- provide appropriate medical care;
- meet safeguarding responsibilities;
- demonstrate reasonable adjustments;
- support EHCP arrangements;
- administer medication; or
- comply with legal or regulatory requirements.

Duplicate or superseded information should be securely deleted when no longer required.

Where a document has been replaced by a current version, the school should retain the earlier version only where there is a clear reason for doing so.

10. Attendance records

Attendance information will be retained in accordance with statutory requirements and the school's Data Retention Schedule.

The school will ensure that:

- attendance information is accurate;
- access is appropriately restricted;
- information is retained for the required period; and
- obsolete duplicate records are securely deleted.

11. Behaviour and disciplinary records

Behaviour records should be retained where necessary to:

- monitor patterns;
- safeguard pupils;
- support pastoral interventions;
- inform educational provision;
- manage serious incidents;
- comply with statutory requirements; or
- respond to complaints, allegations or legal proceedings.

Routine low-level behaviour information should not be retained indefinitely.

Where behaviour information forms part of a safeguarding matter, the safeguarding retention requirements will take precedence.

Records relating to staff disciplinary matters will be managed in accordance with employment law, the school's relevant policies and the Data Retention Schedule.

12. Complaints

Records relating to complaints will be retained for an appropriate period following conclusion of the complaint.

The retention period will take account of:

- the nature of the complaint;
- any appeal;
- safeguarding considerations;
- potential legal proceedings;
- regulatory requirements; and
- the likelihood that the information will be required to demonstrate how the complaint was handled.

Where a complaint raises a safeguarding concern, the relevant safeguarding retention arrangements will apply.

13. Staff records

The school will retain personnel records only for as long as necessary to meet:

- employment requirements;
- statutory obligations;
- pension requirements;
- payroll and taxation requirements;
- safeguarding requirements;
- equality obligations;
- legal claims;
- audit requirements; and
- other legitimate purposes.

The retention of former employee records will be proportionate.

References, recruitment records, DBS-related information, absence information, appraisal records, disciplinary records and occupational health information may have different retention periods.

The school's Data Retention Schedule will identify the appropriate period for each category.

14. Recruitment records

Information relating to unsuccessful applicants will not normally be retained indefinitely.

Recruitment information will be retained for an appropriate period to:

- demonstrate fair and lawful recruitment;
- respond to queries or complaints;
- meet legal requirements; and
- defend potential claims.

Where an applicant is appointed, relevant recruitment information will be incorporated into the employee's personnel record where appropriate.

DBS information will be handled in accordance with current DBS guidance and the school's safer recruitment arrangements.

15. Governor records

Records relating to governors and governance will be retained where necessary to demonstrate:

- governance decisions;
- statutory compliance;
- declarations and interests;
- attendance;
- financial decisions;
- committee work;
- policy approval; and
- other governance responsibilities.

The school will distinguish between records that form part of the official governance record and temporary working documents.

16. Financial records

Financial records will be retained for the period required by:

- legislation;
- HMRC requirements;
- local authority requirements;
- audit requirements;
- funding conditions;
- grant conditions; and
- the school's financial procedures.

Records will be securely disposed of once the relevant retention period has expired.

17. Emails

Emails are records where they document decisions, actions, advice, transactions or other information that the school needs to retain.

The school will not retain every email indefinitely.

Staff should:

- delete routine correspondence when it is no longer required;
- retain emails forming part of an official record in an appropriate system;
- avoid using personal email accounts for school business;
- file important emails with the relevant record where appropriate; and
- securely delete unnecessary emails.

An email inbox should not be treated as a permanent records archive.

18. Photographs and videos

Photographs and videos will be retained only for as long as there is a legitimate reason to retain them.

This may include:

- educational purposes;
- assessment;
- safeguarding;
- school records;
- displays;
- newsletters;
- website content;
- social media;
- publicity;
- events and performances.

Images should be periodically reviewed and deleted where no longer required.

Where images are retained for historical or archival purposes, the school will consider whether continued retention is justified and whether individuals remain identifiable.

Photographs and videos containing safeguarding-sensitive information must be handled in accordance with safeguarding requirements.

19. CCTV

CCTV footage will be retained only for as long as necessary for the purpose for which it was collected.

The school will operate an appropriate retention period reflecting:

- security requirements;
- the nature of the CCTV system;
- available storage;
- safeguarding needs; and
- the need to investigate incidents.

Where footage is required for an investigation, complaint, safeguarding matter or legal proceedings, it may be preserved beyond the normal retention period.

Once the relevant matter has concluded, the footage will be deleted when it is no longer required.

20. Filtering and monitoring records

Filtering and monitoring systems may generate records relating to users' online activity.

The school will retain such information only for as long as necessary to:

- support safeguarding;
- investigate incidents;
- identify patterns;
- meet legal or regulatory requirements; or
- manage the school's systems.

Routine monitoring data should not be retained indefinitely.

Where monitoring information identifies a safeguarding concern, the relevant information will be transferred to the appropriate safeguarding record and retained in accordance with safeguarding requirements.

21. AI and automated systems

Where the school uses AI or other automated systems that process personal data, information will be retained in accordance with:

- the purpose of the processing;
- the provider's contractual arrangements;
- the school's Data Retention Schedule;
- applicable data protection requirements; and
- any DPIA or risk assessment.

Staff must not retain personal data within an AI system simply because the system permits it.

Where an AI provider retains prompts, inputs or outputs, the school must understand and appropriately manage those retention arrangements before using the system with personal data.

22. Cloud systems and third-party providers

Where records are held by a third-party provider on behalf of the school, the school remains responsible for ensuring appropriate retention arrangements.

Contracts and data processing agreements should specify, where appropriate:

- retention periods;
- deletion requirements;
- return of information;
- backup arrangements;
- sub-processors;
- security;
- access;
- data breaches; and
- arrangements at the end of the contract.

When a contract ends, the school will ensure that personal data is returned or securely deleted as required.

23. Legal holds and extended retention

Information may need to be retained beyond its normal retention period where there is:

- actual or anticipated legal action;
- an ongoing investigation;
- a safeguarding concern;
- an unresolved complaint;
- an insurance claim;
- an audit;
- a regulatory investigation;
- a police investigation; or
- another legitimate reason requiring preservation.

Where a **legal hold** or equivalent instruction is issued, relevant information must not be deleted until the hold is lifted.

Staff must follow instructions from the Headteacher, DPO or other authorised person concerning preservation of records.

24. Archiving

Some information may have long-term historical or evidential value.

Before information is archived, the school will consider:

- whether continued retention is necessary;
- whether personal data can be minimised;
- whether anonymisation is possible;
- who requires access;
- how the information will remain secure; and
- whether the archive has an appropriate purpose.

Archiving must not be used as a way of avoiding normal deletion requirements.

25. Secure disposal

When information reaches the end of its retention period, it will be securely disposed of.

Paper records

Confidential paper records must be:

- shredded using an appropriate cross-cut shredder; or
- disposed of through an approved confidential waste provider.

Electronic records

Electronic records must be securely deleted from relevant systems where appropriate.

Where devices are disposed of, the school will ensure that personal data is securely erased before disposal, reuse or recycling.

Removable media

USB devices, external drives and other removable media must be securely erased or physically destroyed where appropriate.

Cloud systems

Information stored with third-party providers must be deleted in accordance with contractual and technical arrangements.

26. Backups

Backups may contain information that has been deleted from active systems.

The school will maintain appropriate backup arrangements for business continuity and disaster recovery.

Where technically practicable, deleted information will cease to be available through normal backup restoration processes within an appropriate period.

Backups must not be used as an alternative archive for information that has reached the end of its retention period.

27. Data breaches and retention

Where information is accidentally retained, disclosed, lost or destroyed contrary to this policy, the incident must be reported in accordance with the school's **Data Protection Policy and Data Breach Procedure**.

Staff must report concerns immediately rather than attempting to conceal or rectify a significant incident without advice.

28. Responsibilities

Governing Body

The Governing Body will:

- approve this policy;
- receive appropriate assurance regarding information governance;
- ensure that appropriate arrangements are in place; and
- monitor significant data protection risks.

Headteacher

The Headteacher will:

- implement this policy;
- ensure appropriate systems are in place;
- ensure staff understand their responsibilities;
- oversee compliance; and
- work with the DPO.

Data Protection Officer

The DPO will:

- advise on retention requirements;
- support the development of the Data Retention Schedule;
- advise on complex retention decisions;
- support data protection compliance;
- advise on data breaches;
- monitor compliance; and
- provide appropriate assurance.

DSL

The Designated Safeguarding Lead will oversee retention decisions concerning safeguarding records, with advice from the DPO where necessary.

Staff

All staff must:

- follow the Data Retention Schedule;
- avoid retaining unnecessary information;
- store records appropriately;
- securely dispose of information when authorised;
- preserve records when instructed;
- report data protection concerns; and
- seek advice when uncertain.

29. Training and awareness

Staff will receive appropriate information and training regarding:

- data protection;
- information security;
- retention;
- secure disposal;
- safeguarding records;
- data breaches;
- email management;
- digital systems;
- AI; and
- relevant school procedures.

Training will be refreshed as necessary.

30. Monitoring and review

The school will monitor compliance through:

- periodic review of the Data Retention Schedule;
- data protection audits;
- review of data breaches;
- review of third-party processors;
- review of electronic systems;
- review of paper records;
- secure disposal records;
- staff training;
- DPO advice and assurance; and
- governor oversight.

This policy will be reviewed annually or sooner where legislation, statutory guidance or school systems change.

Appendix 1 – Data Retention Schedule

The following schedule provides the school's operational starting point. Where a statutory or regulatory retention requirement changes, the school will update the schedule accordingly.

Record / Information	Indicative retention	Trigger / notes
Pupil records / educational record	In accordance with current DfE/education records management requirements	Usually linked to pupil leaving school
Safeguarding / child protection records	In accordance with current safeguarding and records management requirements	Retain separately/securely; safeguarding needs may require extended retention
Attendance records	In accordance with statutory requirements	From relevant academic/attendance year
Admissions records	In accordance with education records management requirements	Review following completion of admissions process
Assessment records	In accordance with DfE requirements and school assessment arrangements	Retain where educationally/statutorily necessary
SEND / EHCP records	In accordance with pupil-record and SEND requirements	Consider continuing educational/legal need
Medical / medication records	In accordance with applicable health, safeguarding and records management requirements	Retain securely
Accident / incident records	In accordance with statutory, insurance and records management requirements	Longer retention may apply to serious incidents
Behaviour records	Normally for as long as educational, safeguarding or legal purpose requires	Safeguarding records follow safeguarding retention
Complaints	Normally in accordance with the school's complaints records retention period	Longer where legal/safeguarding matters remain live
Exclusions / suspensions	In accordance with education records management requirements	Retain as part of pupil record where appropriate
Child-on-child abuse records	In accordance with safeguarding requirements	Treat as safeguarding information

Record / Information	Indicative retention	Trigger / notes
Staff personnel records	Appropriate employment/records-management period	From end of employment where relevant
Payroll records	In accordance with HMRC requirements	Financial year / statutory period
Pension records	In accordance with pension requirements	May require extended retention
Recruitment – unsuccessful applicants	Normally a limited period following recruitment	Longer only where justified
DBS information	In accordance with DBS guidance and safer recruitment arrangements	Do not retain unnecessary copies
Staff disciplinary records	In accordance with employment and records-management requirements	Consider legal claims and safeguarding
Appraisal records	Normally for the period necessary to manage employment and demonstrate appraisal arrangements	Review after employment ends
Governor records	In accordance with governance records-management requirements	Official governance records may require long-term retention
Minutes of Governing Body meetings	Permanent / archival where appropriate	Official governance record
Financial records	In accordance with HMRC, audit, funding and financial requirements	Financial year trigger
Invoices / purchase records	In accordance with financial requirements	Financial year trigger
Contracts	Duration of contract plus appropriate post-contract period	Longer if legal claim remains possible
Data processing agreements	Contract period plus appropriate post-contract period	Retain evidence of compliance
Data breach records	In accordance with UK GDPR/ICO requirements and school records management	Keep record of breaches and decisions

Record / Information	Indicative retention	Trigger / notes
Subject Access Requests	In accordance with records-management requirements	Retain request and response evidence
Freedom of Information requests	In accordance with records-management requirements	Retain decision and response evidence
Privacy notices / policies	Current version plus previous versions where required	Retain evidence of historical compliance
CCTV footage	Shortest period necessary for stated purpose	Preserve longer where required for investigation
Filtering and monitoring logs	Only as long as necessary for safeguarding/system purposes	Safeguarding concerns transferred to safeguarding record
Photographs / videos	While there is a legitimate educational, operational, publicity or archival purpose	Review periodically
Website content	While current; archive where required	Review regularly
Emails	According to content and purpose	Important records should be filed appropriately
Visitor records	Appropriate short operational period	Longer where safeguarding/security incident requires
Premises/security records	According to operational, insurance and legal requirements	Review regularly
Training records	In accordance with employment, safeguarding and compliance requirements	Longer where evidence of statutory training is required

Important: This schedule is a controlled document and must be reviewed against current DfE, ICO, HMRC, safeguarding, employment and other applicable requirements before each annual policy review.

Appendix 2 – Staff Retention Checklist

Before keeping information, ask:

1. Why am I keeping this?
Is there a clear educational, safeguarding, legal or operational reason?

2. Do I need the whole document?
Could unnecessary personal information be removed?

3. Is this the official record?
If it is, store it in the correct school system rather than a personal folder or inbox.

4. How long does it need to be kept?
Check the Data Retention Schedule.

5. Is there a safeguarding or legal reason to keep it longer?
If so, seek advice before deleting it.

6. Can it now be securely deleted?
If the retention period has expired and there is no reason for continued retention, dispose of it securely.

When in doubt, ask the DPO before deleting information that may form part of an official, safeguarding or legal record.

Appendix 3 – Relationship with the Data Protection Policy

This policy should be read alongside the school's **Data Protection Policy**.

The Data Protection Policy establishes the school's overall approach to:

- lawful processing;
- data security;
- data sharing;
- individual rights;
- data breaches;
- privacy;
- DPIAs;
- AI;
- CCTV;
- filtering and monitoring; and
- accountability.

This Data Retention Policy provides the specific framework for deciding **how long information should be kept and how it should be disposed of**.

Where the two documents appear to conflict, the school will seek advice from the Data Protection Officer and follow the applicable statutory requirement.