



Data Retention Policy

Last Reviewed	September 2026
Next Review Date	September 2027
Review Calendar	Annually

Contents

1. Purpose and scope
2. Legal and regulatory framework
3. Principles for retaining records
4. Roles and responsibilities
5. Annual information audit and retention review
6. Secure storage, archiving and access
7. Secure destruction and destruction log
8. Legal holds, complaints, investigations and litigation
9. Transfer of pupil and safeguarding records
10. Email, messaging and digital systems
11. Photographs, video, CCTV, filtering and monitoring
12. Artificial intelligence and EdTech
13. Retention schedule
14. Monitoring and review

1. Purpose and scope

Norbury Manor Primary School has a responsibility to create, maintain, use, retain and dispose of records appropriately. This policy sets out the school's approach to records retention and provides a retention schedule for key categories of school information.

It applies to records in any format, including paper files, emails, photographs, video and audio, management information systems, cloud services, learning platforms, shared drives, safeguarding systems, finance and HR systems, and records held on the school's behalf by processors.

The policy should be read alongside the school's Data Protection Policy, privacy notices, Freedom of Information arrangements, safeguarding and child protection procedures, information security arrangements and any relevant Croydon Council requirements.

2. Legal and regulatory framework

The school will manage records in accordance with applicable legislation and current guidance. This includes, where relevant:

- UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018;
- the Data (Use and Access) Act 2025, which amends and builds on the UK data protection framework;
- Freedom of Information Act 2000;
- Education (Pupil Information) (England) Regulations 2005;
- School Attendance (Pupil Registration) (England) Regulations 2024;
- Limitation Act 1980;
- Keeping Children Safe in Education 2026 and Working Together to Safeguard Children 2026;
- Department for Education guidance on data protection in schools, including record keeping and management;
- relevant employment, tax, pension, health and safety, safeguarding and financial legislation;
- Information and Records Management Society (IRMS) good-practice guidance, where appropriate.

Where a statutory requirement, court order, inquiry, local authority requirement or other binding instruction requires a longer retention period than this schedule, that requirement will take precedence.

3. Principles for retaining records

The school follows the UK GDPR storage limitation principle: personal data will be kept in identifiable form for no longer than is necessary for the purpose for which it is processed.

For each category of information, the school will consider:

- why the information is held and the lawful basis for processing it;
- whether legislation sets a minimum or specific retention period;
- the school's operational, safeguarding, accountability, audit and evidential needs;
- whether another organisation becomes responsible for the record after it is transferred;
- whether the information can be anonymised or depersonalised instead of retained in identifiable form;
- the sensitivity of the information and the risk created by retaining it;
- whether a complaint, investigation, safeguarding matter, insurance claim, legal claim or inquiry requires destruction to be suspended.

Retention periods are minimum/normal periods unless the schedule says otherwise. Records must not automatically be retained indefinitely simply because storage capacity is available.

4. Roles and responsibilities

Governing Body

The governing body has oversight of the school's compliance with data protection and records-management obligations and approves this policy.

Headteacher

The Headteacher is responsible for ensuring that effective records-management arrangements operate across the school and that staff understand their responsibilities.

Data Protection Officer (DPO)

The DPO advises on data protection compliance, retention and disposal, monitors the school's arrangements and should be consulted where a retention decision presents significant privacy or legal risk.

School Business Manager / designated records lead

The designated records lead coordinates the retention schedule, annual review, archiving and destruction arrangements, maintains appropriate destruction records and liaises with the DPO and relevant record owners.

All staff and governors

All staff and governors must store records in approved locations, follow the retention schedule, avoid unnecessary duplication, transfer important emails or messages into the appropriate record system, and never destroy records that are subject to a legal hold or active investigation.

5. Annual information audit and retention review

At least annually, the school will review the personal data and other records it holds. The review will cover paper records, databases, online systems, cloud services, photographs, videos, emails and records held by processors.

The review should identify information that must be retained, securely destroyed, anonymised, archived, transferred or corrected. Decisions about significant retention periods should be reflected in the school's Record of Processing Activities (ROPA) where appropriate.

6. Secure storage, archiving and access

Records must be stored securely, with access limited to those who need the information for their role. Sensitive records, including safeguarding, SEND, health and HR information, require enhanced access controls.

Records selected for permanent or long-term historical preservation should be clearly identified and archived separately from routine operational records. Archiving must not be used as a reason to keep all records indefinitely.

Backups are for disaster recovery and are not a substitute for an active retention process. Where technically possible, deletion from live systems should flow through to backups in accordance with the school's and supplier's backup lifecycle.

7. Secure destruction and destruction log

When records reach the end of their retention period, they must be reviewed before destruction. Destruction must be postponed where there is a legal hold, active complaint, safeguarding investigation, audit, insurance matter, litigation or other documented reason to retain the record.

Confidential paper must be cross-cut shredded or destroyed by an approved confidential-waste contractor. Electronic information must be securely deleted or rendered irretrievable. Storage media must be securely sanitised or physically destroyed where appropriate.

Where an external contractor destroys confidential records, the school will use an appropriately vetted provider and retain suitable evidence or a certificate of destruction.

The school will maintain a destruction log for significant records. It should record:

- a brief description of the records;
- the relevant date range or number of files/boxes;
- the retention rule applied;
- the date of destruction;
- the person who authorised destruction;
- the method/provider used where relevant.

8. Legal holds, complaints, investigations and litigation

Normal destruction must stop immediately for any record that may be relevant to an actual or reasonably anticipated legal claim, safeguarding investigation, complaint, disciplinary process, regulatory investigation, police enquiry, insurance claim, public inquiry or information-rights request.

The DPO, Headteacher or other authorised senior leader will decide when the hold can be lifted and the normal retention period resumed.

9. Transfer of pupil and safeguarding records

The school retains the primary pupil record while the child attends Norbury Manor Primary School. When a pupil transfers to another maintained school or academy, the appropriate pupil record will be transferred securely to the receiving school in accordance with statutory requirements and DfE guidance.

The school should normally retain necessary MIS data for two terms after a pupil leaves to support statutory reporting and operational requirements.

Child protection files must be transferred securely and separately from the main pupil file. The school will retain evidence of transfer rather than an unnecessary duplicate of the full safeguarding file, unless there is a documented reason to retain particular information.

Where Norbury Manor is the last known school or no onward destination is identified, records will be retained in accordance with the schedule below and current DfE guidance.

10. Email, messaging and digital systems

Email and messaging systems are communication tools, not permanent filing systems. There is no single retention period for every email. Retention is determined by the content and purpose of the message.

Emails or messages that form part of a pupil, safeguarding, HR, finance, complaint, governance or other substantive record must be saved to the appropriate approved record system and retained for the period applying to that record. Routine, duplicate and transitory messages should be deleted when no longer needed.

This replaces the previous blanket five-year retention period for all emails.

11. Photographs, video, CCTV, filtering and monitoring

Photographs and video will be retained according to their purpose and the lawful basis for processing. Routine identifiable images should not be kept indefinitely. Where consent is the lawful basis, the school will respect withdrawal of consent for future use, subject to any lawful reason that requires retention.

A small number of images may be selected for the permanent historical archive where there is a clear archival purpose and appropriate safeguards.

CCTV is normally retained for a short period and then overwritten. Norbury Manor's operational retention period is one calendar month unless footage has been isolated because it is required for a safeguarding matter, incident, complaint, investigation, insurance claim or legal process.

Filtering and monitoring alerts, reports and logs will be retained according to safeguarding, security and evidential need. Where an alert becomes part of a safeguarding concern, the relevant information must be stored and retained as part of the safeguarding record rather than relying only on the filtering system.

12. Artificial intelligence and EdTech

The school will not use AI or EdTech platforms as informal long-term repositories for personal information. Before procuring or using systems that process personal data, the school will consider the supplier's retention, deletion, backup and account-closure arrangements and ensure that contractual terms support the school's retention requirements.

Personal data entered into an approved AI or EdTech service remains subject to the same retention, security, transparency and deletion requirements as personal data held elsewhere. Staff must not enter personal or sensitive data into unauthorised AI services.

13. Retention schedule

The schedule below sets the school's normal retention periods. Where a record is covered by a more specific statutory requirement, local authority instruction or legal hold, the longer or binding requirement applies. 'Current year' means the current academic or financial year as appropriate.

13.1 Workforce and employment records

Record / information	Retention period	Action / notes
Unsuccessful recruitment applications/interview records	6 months after appointment decision	Destroy securely unless there is a documented reason to retain longer; talent-pool retention requires an appropriate lawful basis and clear notice.
Successful candidate recruitment records	Transfer relevant records to personnel file; retain with personnel file	Avoid keeping duplicate recruitment copies.
Personnel file / employment records	6 years after employment ends	Securely destroy after review, unless a longer statutory or legal-hold period applies.
Contracts and changes to terms	6 years after employment ends	Usually retained within personnel file.
Right-to-work evidence	Normally 2 years after employment ends	Follow current Home Office requirements; retain only necessary evidence.
DBS certificate copies	No longer than 6 months after recruitment decision	Record the required check/outcome on the SCR; securely destroy certificate copy unless exceptional circumstances justify temporary retention.
Payroll/pay records	3 years from end of relevant tax year (minimum)	Longer finance/LA requirements may apply; follow the longer requirement.
Maternity pay records	3 years after end of tax year in which maternity pay period ends	Securely destroy.
Appraisal/performance records	Current year plus 6 years / or 6 years after employment ends where part of personnel file	Review for duplication and relevance.
Staff safeguarding training records	Date of training plus 40 years where retained for safeguarding evidential purposes	Review against current safeguarding/IRMS guidance.
Safeguarding allegations against staff - substantiated, unfounded or unsubstantiated	Until normal retirement age or 10 years from allegation, whichever is later	Keep the required clear summary and outcome. Review before destruction.
Safeguarding allegations found malicious or false	Remove from personnel record unless the individual consents to retention	Follow KCSIE 2026 and safeguarding advice.

13.2 Pupil, curriculum, attendance and educational visit records

Record / information	Retention period	Action / notes
Primary pupil record	Until pupil leaves Norbury Manor Primary School	Transfer securely to receiving school. Keep necessary MIS data for 2 terms after leaving for reporting/operational purposes.
Pupil record where Norbury Manor is the last known school / no destination	Until pupil's 25th birthday, then review	Securely destroy unless a longer safeguarding/legal reason applies.
Admission register	6 years from admission date (statutory minimum)	School may retain a secure archival/statutory copy where justified.
Attendance register	6 years from date of entry	Updated from the previous 3-year period to reflect the 2024 registration regulations.
Absence correspondence/evidence	Current academic year plus 2 years, unless needed for enforcement/safeguarding	File significant information in the relevant pupil/safeguarding record where appropriate.
Assessment and examination results - school copy	Current year plus 6 years where needed for accountability/evidence	Anonymised trend data may be retained longer.
Curricular records / class records	At least 1 year; normally current year plus 1 year	Destroy when no longer required for teaching/accountability.

Record / information	Retention period	Action / notes
Pupil work	Current academic year, unless selected for assessment evidence or archive	Return to pupil or securely dispose of as appropriate.
SEND records / EHCP information	Transfer with pupil record to receiving school; if no transfer, retain in line with pupil/safeguarding need and review up to DOB + 31 years where EHCP-related liability requires it	No separate universal statutory SEND retention period; avoid duplicate copies once responsibility transfers.
Medical/health administration records	For operational need while pupil attends; significant records retained with pupil record as appropriate	Specific statutory health records may require longer.
Educational visits records	10 years from date of visit	If an incident occurs, retain relevant permission and incident records with the pupil record for the applicable longer period.
Trip consent/permission - routine visit with no incident	Until visit is complete and no longer required; normally end of academic year	The central visit record is retained for 10 years.
Restrictive intervention incident record	Retain in pupil record according to the nature of the incident; central log retained on a documented risk-led basis	From April 2026, maintain both the individual record and central oversight record.

13.3 Safeguarding and child protection records

Record / information	Retention period	Action / notes
Child protection file	Until child's 25th birthday	Transfer separately to new school where applicable; securely dispose at end of period.
Child protection file relating to child sexual abuse	Until child's 75th birthday	Reflects current DfE guidance following IICSA recommendations.
Safeguarding chronology / concern records	Retain with child protection file	Do not keep fragmented duplicate safeguarding records in general folders.
Records of referrals to children's social care / police	Retain with safeguarding file where relevant	Transfer securely with safeguarding file when pupil moves.
Low-level concerns about staff	Retain and review in accordance with the school's safeguarding policy and KCSIE; normally at least until employment ends, with longer retention where needed for safeguarding patterns/evidence	Keep separate from routine personnel material as appropriate and review proportionately.

13.4 Finance, contracts and funding records

Record / information	Retention period	Action / notes
Contracts	6 years from last payment / completion	Longer period may apply to deeds or where Croydon requirements specify.
Invoices, receipts, purchase orders and requisitions	Current financial year plus 6 years	Securely destroy after audit/legal requirements expire.
VAT records	6 years from financial year end	Statutory/tax requirement.
Annual accounts	Current year plus 6 years	Retain final approved accounts longer if selected for archive.
Budgets and working papers	Life of budget plus 3 years	Retain final approved financial records as required.
School fund records and bank statements	Current year plus 6 years	Securely destroy.

Record / information	Retention period	Action / notes
Free school meal funding records	Current year plus 6 years where used as funding evidence	Avoid retaining unnecessary supporting personal data.
Pupil Premium funding records	Pupil leaves plus 6 years where required as funding/audit evidence	Review whether aggregated evidence can replace identifiable data.
Lettings records	Current financial year plus 6 years	Longer where an unresolved claim exists.
Insurance records/claims	Current year plus 6 years after closure of matter, or insurer requirement if longer	Apply legal hold to active claims.

13.5 Governance, policies and complaints

Record / information	Retention period	Action / notes
Instrument of Government	Life of school / permanent	Archive.
Signed governing body minutes - principal set	Permanent / life of school	Archive securely.
Agendas supporting principal minutes	Store with principal minutes where appropriate	Duplicate copies can be destroyed after meeting/business need.
Governor attendance records	6 years after relevant period / last entry	Securely destroy after review.
Governor appointment/term-of-office records	6 years after appointment ceases	Securely destroy.
Register/declarations of business interests	6 years after appointment ceases	Published versions may be replaced when updated; retain governance record.
Governor training records	6 years after appointment ceases	Securely destroy.
Policies	Current version plus previous version for 6 years unless a longer evidential need applies	Key historic policies may be selected for archive.
Headteacher/SLT reports to governors	Minimum 6 years where part of governance record	Permanent retention may be appropriate for significant strategic reports.
Complaints records	Normally current year plus 6 years after closure	Safeguarding, negligence, litigation or other significant matters may require longer; apply legal hold where relevant.

13.6 Health, safety, premises and visitors

Record / information	Retention period	Action / notes
Health and safety risk assessments	Life of assessment plus 3 years; consider 6 years where evidential need applies	Retain superseded versions where relevant to incidents/claims.
Fire risk assessments	Life of assessment plus 6 years	Securely destroy after review.
Accident records - adults	3 years from date of accident / last entry as applicable	Active claims require longer retention.
Accident records involving pupils	Retain relevant incident information in pupil record; normally until pupil reaches 21 where limitation risk requires	Apply longer period where a claim or safeguarding issue exists.
Health surveillance records	40 years	For records subject to statutory occupational-health requirements.
COSHH control-system test/examination records	5 years	Securely destroy after period.

Record / information	Retention period	Action / notes
Asbestos/long-latency exposure records	Follow applicable statutory requirement, commonly 40 years for relevant health surveillance	Seek competent H&S advice for specific record types.
Visitors/signing-in records	Normally current year plus 3 years; longer where safeguarding/security need justifies	Minimise retained personal data.

13.7 Digital records, privacy, CCTV and information governance

Record / information	Retention period	Action / notes
Routine emails and messages	Delete when no longer needed	Substantive records must be filed and inherit the retention period of the relevant record category.
Privacy notices	Current version plus 6 years	Retain evidence of historic wording provided to data subjects.
Consent records	For duration of processing plus sufficient period to evidence consent/withdrawal; normally up to 6 years after processing ends	Do not treat consent as permanent.
CCTV footage	1 calendar month	Overwrite unless isolated for an incident, safeguarding matter, complaint, insurance claim or legal process.
Filtering and monitoring routine logs/reports	According to operational/security need and supplier configuration; review at least annually	Relevant safeguarding alerts must be retained within safeguarding records.
Photographs/videos - routine school use	For the period needed for the stated purpose and while the lawful basis remains valid	Review regularly; delete when no longer needed.
Photographs/videos selected for school history/archive	Permanent where there is a documented archival purpose	Use appropriate safeguards and access controls.
Website/social-media source files	While published/needed, then review	Remove outdated personal data; archived web content should be proportionate.
Data breach log	Minimum 6 years after closure unless risk/legal advice requires longer	Keep sufficient record to demonstrate accountability.
Subject access request / information-rights case file	3 years after closure, or longer where complaint/litigation is ongoing	Retain decision trail and disclosure record proportionately.
DPIAs and significant data-protection decisions	Life of processing/activity plus 6 years	Retain earlier versions where they evidence decisions.
ROPA / information asset register	Current version plus previous versions as needed for accountability, normally 6 years	Review at least annually.

14. Monitoring and review

The DPO and designated records lead will monitor implementation of this policy. The retention schedule will be reviewed at least annually and sooner where legislation, DfE guidance, Croydon Council requirements, safeguarding guidance, technology or school processes change.

The school will carry out an annual information audit and will provide appropriate training so that staff understand secure storage, retention, transfer and destruction requirements.

This policy is approved by the governing body.

Key reference documents

- Department for Education: Data protection in schools - Record keeping and management (updated July 2026).

- Department for Education: Data protection in schools - The Data (Use and Access) Act 2025.
- Department for Education: Keeping Children Safe in Education 2026.
- Department for Education: Working Together to Safeguard Children 2026.
- Department for Education: Retention schedule for data processed by DfE (updated September 2026).
- Information Commissioner's Office guidance on storage limitation, security and disposal.
- IRMS Information Management Toolkit for Schools and Academies, where accessible and applicable.