Southbury Primary School

Retention and Disposal Schedule

September 2026

Document control	Details
School	Southbury Primary School, Swansea Road, Enfield, EN3 4JG
Document owner	Rebecca Panteli, Headteacher
DPO	Enfield Council Data Protection Officer – Andrea Kilby
Version	November 2026
Approved by	Bradley Jones, Chair of Governors
Approval date / next review	September 2027
Related documents	Privacy Notice; DPIA; Record of Processing Activities (RoPA); Data Breach Procedure; Information Security Policy; Safeguarding and Online Safety policies; contracts and processor register

1. Purpose and scope

This schedule sets out how long Southbury Primary School keeps records created or received in carrying out its functions as a school and employer, and what action must be taken when the retention period ends. It applies to information in every format, including paper files, emails, databases, cloud services, photographs, video, audio, messaging platforms, removable media and records held by service providers on the school's behalf.

The schedule supports data protection, records management, safeguarding, accountability and freedom of information obligations. It does not authorise routine destruction where a record is subject to a legal hold, investigation, complaint, safeguarding matter, audit, claim, information request or other preservation requirement.

2. Responsibilities

- All staff are responsible for managing records in accordance with this schedule and using approved school systems and storage locations.
- Record owners / subject leaders must identify records they create, ensure they are stored securely and arrange timely review and disposal.
- The Headteacher or delegated senior leader is responsible for authorising the schedule and overseeing its implementation.

- The school's Information Governance Lead / designated administrator should maintain the destruction log and coordinate the annual review.
- The Data Protection Officer (DPO) should be consulted on uncertain retention periods, high-risk records, changes to processing and proposed departures from this schedule.
- IT support and service providers must support secure deletion, retention settings, backup management and the return or deletion of data at contract end.

3. How to apply the schedule

- Identify the record category and use the retention period stated in the relevant row.
- Calculate the period from the stated trigger (for example, date of last entry, date of leaving, end of employment or closure of a case). Do not calculate from the date a file happens to be moved or archived unless the row says so.
- Where the schedule says "review", a named record owner must assess whether there is a documented continuing need and record the decision and new review date.
- Where records are transferred to another school or authority, use a secure, documented transfer process and retain only the information the school still needs.
- Do not keep records indefinitely "just in case". If a longer period is needed, document the purpose, lawful basis, rationale, authorisation and review date.
- Where two retention rules could apply, identify the record's primary purpose and consult the DPO before disposal. Do not automatically apply the longest period to every item in a mixed file.

4. Legal holds and exceptions

Suspend routine destruction where records may be relevant to actual or anticipated litigation, a safeguarding investigation, a complaint, an employment dispute, an audit, an insurance claim, a police or regulatory enquiry, a freedom of information request or a data subject rights request. The relevant senior leader should record the hold, the records affected, the reason, the owner and the date for review. Resume normal disposal only when the hold is formally lifted.

A request for access or erasure does not automatically require the school to destroy records. Apply the relevant legal rules and exemptions and seek DPO advice.

5. Secure disposal and transfer

- Paper records containing personal or confidential information must be cross-cut shredded or disposed of through an approved confidential-waste provider. They must not be placed in ordinary recycling or general waste.
- Electronic records must be securely deleted from the live system and, where technically and contractually possible, from associated storage, exports and removable media. Backup copies should expire through documented backup cycles; do not promise immediate deletion from immutable backups if this is not technically possible.
- Where an external provider destroys records, obtain and retain a certificate or other evidence of destruction where available.
- Maintain a destruction log recording the record category, date range / identifier, quantity or volume, retention rule, date of destruction, method, authorising officer and provider / certificate reference.
- Transfer records to an archive only where there is an agreed archival arrangement and a documented decision. The previous schedule contains references to transfer to Archives, but some entries have no archive contact; confirm the correct Enfield archive arrangements before transfer.
- Securely transfer pupil records to the receiving school using the agreed process. Record the transfer date, recipient and method.

6. Retention schedule

The periods below are a working framework. Entries marked “DPO confirmation required” must be checked before this schedule is approved. “Current year” means the current academic or financial year as specified by the relevant record owner; the school must define the convention consistently for each record series.

6.1 Governance and governors

Record category	Retention period / trigger	Action at end of period	Notes / status
Governing body minutes – signed master copy	Permanent while school operates; retain securely. Confirm archival transfer arrangements when no longer required.	Transfer to agreed archive / permanent preservation where appropriate.	Confirm with Enfield Archives and governance lead.
Copies of minutes, agendas and routine meeting papers	Annual governors' report: 10 years (DfE guidance). For minutes and other governance records, confirm local governance / archive requirements; do not apply this period automatically.	Secure destruction.	Check whether papers form part of the official decision record.
Reports considered by governing body	Meeting date + 6 years as a working period; review for significant or enduring decisions.	Destroy or transfer selected records to archive under agreed arrangements.	Confirm local governance guidance.
Instrument of Government / constitutional records	Permanent while school operates; retain superseded versions where needed to evidence governance history.	Archive / permanent preservation where appropriate.	Confirm archival arrangements.
Policies and procedures	Current version while in force; superseded versions retained for 6 years after replacement as a working period, or longer where they evidence a decision, complaint or legal requirement.	Secure destruction or archive selected significant versions.	Keep version and approval history.
Governor declarations of interest, attendance and appointment records	DPO confirmation required; distinguish statutory publication / governance records from personal supporting documents.	Secure destruction when period expires.	Check current governance requirements.
Complaints files	DPO confirmation required; retain according to complaint type, seriousness, appeal / litigation risk and any safeguarding implications.	Secure destruction after approved period and any hold ends.	Do not apply one period to all complaints.
Annual reports and statutory governance returns	DPO confirmation required; check current statutory and archive requirements.	Destroy or archive as appropriate.	Old reference to DfES is obsolete.

6.2 School leadership and management

Record category	Retention period / trigger	Action at end of period	Notes / status
Senior leadership / management meeting minutes	Meeting date + 5 years as a working period; review if needed for a decision, dispute or inspection evidence.	Secure destruction or archive selected records.	Confirm with DPO / governance lead.
Headteacher / senior leader reports and strategic papers	Report date + 3 years as a working period; significant strategic decisions may require longer retention.	Review, then destroy or archive selected records.	Avoid retaining duplicate working copies.
School development / improvement plans	Superseded / closure + 6 years as a working period.	Review for archive value, then securely destroy or transfer.	Retain evidence supporting significant decisions.
Operational correspondence and administrative files	Normally closure + 3 years; longer only where linked to a defined legal, safeguarding, financial or employment purpose.	Secure destruction.	Apply specific category rules where available.
Log books and records of significant school events	DPO confirmation required; identify whether safeguarding, accident, governance or other specific rules apply.	Review and destroy / archive under the relevant rule.	Avoid a single blanket period for all log books.

6.3 Pupils – admissions, attendance and educational records

Record category	Retention period / trigger	Action at end of period	Notes / status
Admission register	6 years from the admission date (DfE guidance; confirm the register entry / start date used in practice).	Secure destruction or archive where required.	Electronic and paper versions; ensure any duplicate exports are managed.
Attendance register	6 years from the date of entry (DfE guidance).	Secure destruction.	Include electronic records and relevant backup / export arrangements.
Pupil educational record / main pupil file	Transfer securely to the next school when the pupil leaves. Retain any copy only for a documented continuing purpose and period.	Securely transfer; securely destroy school copies when no longer needed.	Check current DfE guidance and local authority transfer process.
Primary pupil record held by receiving / former school	For a primary school, the core pupil record is retained until the pupil leaves and transferred	Secure destruction when approved period ends.	Separate core educational record from safeguarding and specialist records.

Record category	Retention period / trigger	Action at end of period	Notes / status
	to the next school. Any retained copy needs a separate documented justification.		
Letters / evidence relating to pupil absence	DPO confirmation required; align with attendance register and any safeguarding / statutory purpose.	Secure destruction.	Do not confuse the letter with the statutory attendance register.
Exclusion / suspension records	DPO confirmation required; consider statutory review / appeal periods, safeguarding and transfer requirements.	Secure destruction when period and any hold end.	Use current terminology: suspension and permanent exclusion.
Pupil assessment, progress and attainment records	DPO confirmation required; set periods by purpose, including statutory assessment, transfer, school improvement and appeals.	Secure deletion / destruction when no longer needed.	Include Arbor exports, spreadsheets and teacher-held copies.
Internal examination / test results and work samples	DPO confirmation required; retain only for assessment, moderation, appeals and agreed school improvement purposes.	Secure destruction.	Avoid blanket retention of all pupil work.
Public examination / statutory assessment results and certificates	DPO confirmation required; check awarding body and statutory requirements.	Return unclaimed certificates to awarding body where required; securely destroy other records when due.	Primary school assessment records differ from secondary examination records.
Other pupil administrative records	Normally case closure + 3 years as a starting point, unless a more specific category applies; review before disposal.	Secure destruction.	Record the specific purpose and any special category data.

Additional pupil / governance records: DfE guidance specifies records of educational visits are retained for 10 years from the visit date. If an incident occurs, retain permission slips for all pupils and the incident report in the pupil record. Curricular records must be retained for at least 1 year. Confirm whether Southbury creates these records and include them in the local records inventory.

6.4 Safeguarding and child protection

Safeguarding records must be managed separately from routine pupil administration where required, with restricted access and secure transfer. The periods below must be checked against the current DfE guidance, KCSIE, local authority safeguarding procedures and DPO advice before approval.

Record category	Retention period / trigger	Action at end of period	Notes / status
Child protection / safeguarding file	Current DfE guidance: normally until the child's 25th birthday; where the file relates to child sexual abuse, retain until the child's 75th birthday. Confirm current guidance and local safeguarding requirements before adoption.	Secure transfer to receiving school when pupil moves; otherwise secure destruction at end of approved period, subject to holds.	DPO / DSL confirmation required. Record the source and transfer receipt.
Safeguarding referrals and case records not held in the main child protection file	DPO / DSL confirmation required; determine whether they form part of the child protection file or a separate record series.	Secure transfer / destruction under the applicable safeguarding rule.	Do not split a file in a way that loses context.
Allegations against staff	DPO confirmation required. Current DfE guidance includes specific retention rules; verify the applicable period and distinction between substantiated, unsubstantiated, false and malicious allegations.	Secure destruction only after approved period and any hold ends.	Keep separate from routine personnel file where required; consult HR / DPO.
Low-level concerns about adults working with children	DPO confirmation required; align with current KCSIE and local safeguarding procedures.	Secure destruction at end of approved period.	Record rationale, access restriction and any link to a later allegation.
LADO referrals / strategy meeting records	DPO / safeguarding authority confirmation required; establish which organisation is record owner and whether school holds a copy.	Secure destruction / transfer under agreed rule.	Do not assume the school is the sole controller.
Safer recruitment / DBS and vetting records	DPO / HR confirmation required; retain only the permitted information and for the approved period after recruitment decision / check.	Secure destruction; do not retain prohibited DBS certificate details longer than permitted.	Keep a record of check outcome / date where appropriate, not unnecessary certificate copies.

6.5 SEND, inclusion and medical information

Record category	Retention period / trigger	Action at end of period	Notes / status
SEND support records, provision maps, reviews and individual plans	DPO confirmation required; distinguish routine SEND support records from statutory EHC plan / assessment records and safeguarding records.	Secure transfer where needed; secure destruction when no longer necessary.	Old schedule's DOB + 25 / closure + 35 entries require verification; do not carry forward automatically.
Education, Health and Care (EHC) plan and statutory assessment records	DPO confirmation required with local authority SEND team; establish controller, record ownership, transfer and retention responsibilities.	Transfer / retain / destroy under agreed statutory and local authority rules.	Do not assume school retains the authoritative LA file.

Record category	Retention period / trigger	Action at end of period	Notes / status
Medical, allergy, medication and care-plan records	DPO confirmation required; retain while needed for safe care and for an appropriate period after the pupil leaves, based on risk and legal advice.	Secure destruction when no longer required and approved period ends.	Keep current operational information accessible to relevant staff only.
Accident / injury records involving pupils	See Health and Safety section; DPO confirmation required for the record type and age of child.	Secure destruction after approved period and any claim / hold ends.	Cross-reference incident and safeguarding records where relevant.
Accessibility and reasonable adjustment records	DPO confirmation required; retain while adjustment is needed and for a justified period afterwards.	Secure destruction.	Keep sensitive information access restricted.

6.6 Curriculum, teaching and assessment

Record category	Retention period / trigger	Action at end of period	Notes / status
Curriculum plans, schemes of work and subject documentation	Current version while in use; superseded version normally 3 years after replacement as a working period.	Secure destruction or archive significant versions.	Retain only what is needed for curriculum continuity, accountability and review.
Timetables, class lists and routine teaching records	Academic year + 1 year as a working period; review where needed for a complaint, safeguarding or statutory purpose.	Secure destruction.	Class lists may contain sensitive data.
Teacher mark books, assessment spreadsheets and working notes	Academic year + 1 year as a starting point; retain longer only where required for assessment, moderation, appeals or an identified purpose.	Secure deletion / destruction.	Ensure data in Arbor is not duplicated indefinitely in personal drives.
Pupil work and portfolios	Academic year + 1 year as a starting point; retain selected samples only for a documented educational, moderation or archive purpose.	Return to pupil / family where appropriate or securely destroy.	Consider photographs and digital portfolios separately.
Statutory assessment / national test records	DPO confirmation required; check current DfE assessment guidance and any required submission / record keeping.	Secure destruction when period ends.	Do not use the old blanket “current year + 6 years” without verification.
School performance / analysis reports	Normally current year + 3 years as a working period; anonymise or aggregate where identifiable pupil data is no longer needed.	Secure destruction or retain anonymised statistics.	Retain underlying identifiable data only under its own rule.

6.7 Personnel, recruitment and employment

Record category	Retention period / trigger	Action at end of period	Notes / status
Core staff personnel file	6 years from termination of employment for personnel files (DfE guidance); separate records within the file may have different statutory periods and should be reviewed individually.	Secure destruction when each record category reaches end of period.	Old schedule's termination + 7 years must be checked against current employment and limitation requirements.
Payroll, tax, pension and statutory pay records	Pay records: 3 years from the end of the tax year they relate to (DfE guidance). Retirement benefits: minimum 6 years from end of the year in which accounts were signed. Confirm other payroll and pension categories separately.	Secure destruction / provider deletion.	Do not use one period for all salary and pension information.
Timesheets, overtime and absence records	DPO / HR confirmation required; align with payroll, statutory pay and employment record requirements.	Secure destruction.	Separate routine absence data from occupational health records.
Recruitment applications and interview notes – unsuccessful candidates	Unsuccessful recruitment records: 6 months after the recruitment decision as a working period, subject to claim / complaint holds. Confirm with HR / DPO.	Secure destruction.	Keep only records needed to evidence fair recruitment.
Successful candidate recruitment records	Transfer relevant documents to personnel file; retain other recruitment material only for a justified period.	Secure destruction of duplicate / unnecessary material.	Do not retain full application pack indefinitely.
DBS / pre-employment vetting information	Copies of DBS certificates: 6 months from date of recruitment (DfE guidance). Do not retain certificate copies longer unless exceptional circumstances justify it and DPO / HR advice is obtained.	Secure destruction of certificate copies; retain permitted record of check outcome where appropriate.	Old CRB references must be replaced.
Disciplinary, grievance and capability records	DPO / HR confirmation required. For allegations of child protection against a staff member, including unfounded allegations, DfE guidance specifies until normal retirement age or 10 years from the allegation, whichever is later. Other disciplinary records need a separate rule.	Secure destruction after approved period and any hold ends.	Safeguarding-related matters may require separate records and longer periods.

Record category	Retention period / trigger	Action at end of period	Notes / status
Appraisal, performance management and professional development records	Normally employment duration + 2 years as a working starting point; confirm HR / DPO requirements.	Secure destruction.	Do not retain unnecessary sensitive commentary.
Occupational health and health records	DPO / HR confirmation required; apply specific statutory and health-record rules; store separately with restricted access.	Secure destruction under approved category-specific period.	Special category data.
Maternity, paternity, adoption, shared parental and other statutory pay records	DPO / payroll confirmation required; follow current HMRC and statutory pay record requirements.	Secure destruction.	Old statutory references may have changed.
Accident at work / employer liability records	See Health and Safety section; apply incident type, injury severity, limitation and insurance requirements.	Secure destruction when approved period ends.	Serious injury / safeguarding / claim records may need longer retention.
Staff training and safeguarding training records	Employment duration + 6 years as a working starting point; confirm statutory / safeguarding evidence needs.	Secure destruction.	Keep evidence needed to demonstrate required training.

6.8 Health and safety

Record category	Retention period / trigger	Action at end of period	Notes / status
Risk assessments and general health and safety policies	Superseded / expiry + 3 years as a working period; longer if linked to an incident, claim or statutory requirement.	Secure destruction.	Retain current versions and approval history.
Accident records – adults	3 years from the date of the accident (DfE guidance). Accidents involving pupils should also be retained in the pupil record; retain longer where a claim, safeguarding issue or legal hold applies.	Secure destruction after approved period and any hold ends.	Separate reportable incidents and claims.
Accident records – children	DfE guidance says accident records involving pupils should be retained in the pupil record. The school must check whether additional retention is justified for the particular incident, age of child, claim risk or safeguarding context.	Secure destruction after approved period and any hold ends.	Consider child limitation periods and safeguarding context.
RIDDOR reports and supporting evidence	Apply the relevant RIDDOR and HSE requirements to the specific record type; use the 3-year accident record period only where applicable.	Secure destruction when statutory / justified period ends.	Keep evidence of report and investigation.
COSHH assessments and exposure records	COSHH exposure monitoring: DfE guidance lists 5 years; health surveillance records: 40 years. Check the specific substance, exposure and applicable COSHH requirements before disposal.	Secure destruction only after checking applicable regulations.	Do not apply one period to all COSHH documents.
Asbestos management / exposure records	DPO / premises / H&S confirmation required; statutory retention may be long-term and depends on record type.	Secure preservation / transfer to responsible premises owner where appropriate.	Old schedule states 40 years after last action; verify current legal requirement.
Radiation exposure records	DPO / H&S confirmation required; apply the current Ionising Radiations Regulations and HSE retention requirements. Do not rely on the old 50-year period without verification.	Secure preservation / transfer as required.	Old schedule states 50 years; verify current legal requirement.
Fire safety logs, drills and inspections	DPO / H&S confirmation required; set period based on fire safety duties, insurer and local authority requirements.	Secure destruction when approved period ends.	Retain records needed to evidence compliance.

6.9 Finance, procurement and grants

Record category	Retention period / trigger	Action at end of period	Notes / status
Annual accounts and financial statements	6 years from the last payment on the contract (DfE guidance); check contract terms and any legal hold.	Secure destruction or archive where required.	Keep audit trail.
Invoices, receipts, orders, delivery notes and routine accounting records	6 years from the end of the financial year for VAT records (DfE guidance); confirm whether the record is a VAT record or another financial record.	Secure destruction.	Include electronic accounting records.
Contracts – executed under hand / signature	Contract end / expiry + 6 years as a working starting point; confirm contract terms and limitation period.	Secure destruction.	Check data processing terms and deletion at contract end.
Contracts – deeds / under seal	Contract end / expiry + 12 years as a working starting point; confirm legal advice and contract form.	Secure destruction.	Retain longer if dispute / asset / safeguarding implications.
Contract monitoring and supplier performance records	Contract end + 2 years as a working period; longer if needed for disputes, audit or safeguarding.	Secure destruction.	Separate personal data and confidential commercial information.

Record category	Retention period / trigger	Action at end of period	Notes / status
Loans, grants and funding applications	Final payment / grant closure + 6 years as a working starting point; funding agreement may specify longer.	Secure destruction or archive where required.	Check each grant's conditions and audit requirements.
Budget plans, monitoring and forecasts	Financial year end + 3 years as a working period; retain approved budget / accounts evidence under relevant financial rule.	Secure destruction.	Remove unnecessary staff / pupil identifiers.
School fund / petty cash / bank records	Financial year end + 6 years as a working period; confirm financial regulations.	Secure destruction.	Includes bank statements, ledgers and receipts.
Free school meal eligibility and applications	DPO / finance confirmation required; retain eligibility evidence only for the period needed to administer entitlement and meet audit requirements.	Secure destruction.	Separate eligibility records from registers and anonymised meal counts.
Breakfast club, school meals and payment records	Financial year end + 6 years as a working starting point for financial transactions; operational registers may require a shorter period.	Secure destruction.	Distinguish payment evidence from daily attendance / meal counts.

6.10 Premises, property, visitors and CCTV

Record category	Retention period / trigger	Action at end of period	Notes / status
Title deeds, leases and core property ownership records	Permanent while relevant to the school / property; retain or transfer to successor body as appropriate.	Secure transfer / archive.	Keep originals in secure storage.
Building plans, surveys and major works records	For life of building / asset plus an appropriate period; DPO / premises / legal confirmation required.	Transfer to successor premises owner / archive or securely destroy when no longer needed.	Some records have long-term safety value.
Routine maintenance and contractor records	Completion / financial year end + 6 years as a working period; longer where linked to building safety, defects or claims.	Secure destruction.	Check contracts and insurance requirements.
Lettings and booking records	Event / booking + 3 years as a working period; financial records follow finance schedule.	Secure destruction.	Keep incident records separately where needed.
Visitor books / sign-in records	12 months as a proposed school operational period; confirm with DPO / safeguarding lead and review if visitor records are used for safeguarding or security investigations.	Secure destruction.	Minimise data collected and restrict access.
CCTV footage	Set the shortest period that meets the documented purpose; confirm the actual configured period with the DPO. Preserve relevant footage separately for an incident, investigation or legal hold.	Automatic secure deletion; preserve relevant clip under a documented hold.	Display appropriate signage and provide privacy information.
Photographs, video and audio recordings	Retain while there is a defined educational, safeguarding, communications or archival purpose and permissions / lawful basis remain valid; review annually.	Delete or securely archive selected material; remove from platforms when no longer needed.	Set separate rules for public website / social media and internal learning records.
Burglary, theft, vandalism and insurance incident records	Incident closure + 6 years as a working period; longer if claim or legal hold applies.	Secure destruction.	Confirm with insurer.

6.11 IT systems, digital records and communications

Record category	Retention period / trigger	Action at end of period	Notes / status
Emails and electronic correspondence	Apply the retention period for the subject matter; routine transitory messages should be deleted when no longer needed, normally within 12 months as a working practice.	Secure deletion from mailbox / archive in line with system settings.	Do not retain all email indefinitely.
Arbor / MIS data and exports	Apply the retention rule for the underlying record category; delete duplicate exports and local copies when no longer needed.	Delete / securely dispose of exports and manage provider deletion settings.	Confirm provider contract, backups, data location and export arrangements.
Tapestry / EYFS observations and media (if still used)	Apply pupil educational record, image and safeguarding rules according to content; confirm retention and deletion settings.	Transfer / delete under relevant category; verify provider deletion.	Confirm whether Southbury still uses this platform.
Filtering and monitoring logs / alerts	DPO / safeguarding / IT confirmation required; define proportionate period based on alert type and safeguarding purpose.	Secure deletion after approved period; preserve relevant case evidence separately.	Record what is monitored, who can access alerts and retention period.
Cloud storage, shared drives and collaboration platforms	Apply underlying record category; review shared folders and delete duplicate / superseded files.	Secure deletion; confirm provider deletion and backup lifecycle.	Use approved school accounts and access controls.
Website, school social media and newsletters	Retain published content while current; review annually and remove outdated personal information when no longer needed.	Remove from public channels; retain approved archive copy only where justified.	Review children's images and staff details.
System access logs and security logs	DPO / IT confirmation required; set period based on security monitoring, incident detection and system capability.	Secure deletion / automatic expiry.	Document system-specific periods.
Backups and disaster recovery copies	Defined backup rotation / expiry set by IT and provider; not an indefinite archive.	Automatic expiry / secure overwrite in line with documented backup cycle.	Record backup schedule and how deletion requests / holds are handled.

Record category	Retention period / trigger	Action at end of period	Notes / status
AI tools and automated processing records	DPO confirmation required; apply underlying data category and retain prompt / output only where necessary for a defined purpose.	Delete prompts, outputs and uploaded data under provider settings / contract.	Use only approved tools; do not enter identifiable pupil or staff data without authorisation.

6.12 External providers and data held on the school's behalf

The school must maintain a current processor / supplier register. Contracts and data processing terms should specify the provider's instructions, security, sub-processors, international transfers, breach notification, assistance with rights requests, retention, and return or deletion of data at the end of the service. The school must establish how deletion is evidenced and how backups are treated.

Record category	Retention period / trigger	Action at end of period	Notes / status
Data held by processors / cloud suppliers	Same retention rule as the underlying school record unless contract / law requires otherwise.	Provider returns or securely deletes data at contract end; obtain confirmation where appropriate.	Check sub-processors and backup deletion.
Data sharing agreements and processor contracts	Contract expiry + 6 years as a working period; deeds / claims may require longer – confirm with legal / DPO advice.	Secure destruction / archive selected governance records.	Maintain current agreements and version history.
Data breach records and investigation files	DPO confirmation required; retain sufficient records to demonstrate compliance and manage legal / regulatory claims.	Secure destruction after approved period and any hold ends.	Maintain breach register, decisions and evidence.

7. Destruction log

The school should maintain a central destruction log. A suggested template is below. The log should not reproduce unnecessary sensitive details; use a unique reference and concise description.

Date destroyed	Record category / reference	Date range / quantity	Retention rule applied	Method / provider	Authorised by	Certificate / evidence ref
[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

8. Annual review and implementation checklist

- Confirm all record categories created by the school are included, including new systems, online services and paper records.
- Confirm retention periods and legal references with the DPO, HR, finance, safeguarding lead, premises lead and IT support as relevant.
- Check current DfE and ICO guidance and any Enfield Council records management requirements.
- Confirm the schedule matches the school's Privacy Notice, DPIA, RoPA, processor register, data sharing agreements and contracts.
- Identify the owner of each record category and ensure staff know where records should be stored.
- Check secure disposal arrangements for paper, electronic records, backups and third-party providers.
- Train staff and communicate changes; remove obsolete local retention lists and templates.
- Record approval, version, review date and any exceptions.

Review / approval record	Details
Review date	September 2027
DPO advice received	
Consulted roles	
Changes made	
Outstanding actions	
Approved by	
Next review due	