

Records Retention Schedule

Our vision: Templars, a place where everyone belongs. A place where everyone is proud to belong.
A school where everyone is welcomed, feels safe and strives to achieve their full potential.

Our mission: Every child, Every day, Every chance.

Our values: Care, Respect and Honesty.

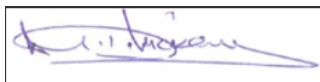
Document Control

Item	Detail
Policy Author	Helen Benarous/Headteacher
Policy Owner	Headteacher
Approval	Governing Board
Date Ratified	Autumn 2026
Review Cycle	Bi- Annually
Next Review Due	Autumn 2028 (or sooner if statutory guidance)

Signatures

Role	Name	Signature	Date
Headteacher	Helen Benarous		16.8.26

Chair of Governors Martin Vickery





Distribution

- Available on the school website
- Available from the school office on request
- Shared with staff on Sharepoint

1. Purpose

Templars Primary School creates and holds records in order to educate and safeguard pupils, employ and support staff, manage the school effectively, meet its statutory responsibilities and provide evidence of its decisions and actions.

Good records management supports:

- effective teaching, safeguarding and pastoral care;
- continuity when pupils or staff move;
- sound decision-making and accountability;
- efficient school administration;
- compliance with legal, regulatory and financial requirements;
- protection of the rights and interests of pupils, families, staff and the school;
- appropriate responses to information rights requests, complaints, investigations and legal proceedings; and
- preservation of records of enduring historical value where appropriate.

This policy establishes the principles by which records are created, managed, stored, accessed, retained, transferred and securely disposed of.

It applies to records in **all formats and locations**, including paper and electronic records, emails, management information systems, safeguarding systems, cloud platforms, SharePoint, photographs, video, CCTV, audio recordings and other digital systems.



2. Scope

This policy applies to all records created, received, maintained or held by or on behalf of Templars Primary School in connection with its functions.

This includes records relating to:

- pupils and former pupils;
- parents and carers;
- safeguarding and child protection;
- SEND and additional needs;
- attendance;
- behaviour;
- teaching, assessment and curriculum;
- staff, recruitment and employment;
- governors and governance;
- finance and procurement;
- health and safety;
- premises and assets;
- complaints;
- correspondence and communications;
- contracts and suppliers; and
- the management and administration of the school.

The policy applies to all employees, governors, volunteers and others who create, receive or manage school records as part of their role.

Records created while carrying out school business remain school records regardless of the device, system or location in which they were created.



3. Legal and Regulatory Framework

The school manages records in accordance with relevant legislation and statutory requirements, including, where applicable:

- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018;
- Data (Use and Access) Act 2025;
- Freedom of Information Act 2000;
- Environmental Information Regulations 2004;
- Education Act 1996;
- Children Act 1989 and Children Act 2004;
- Equality Act 2010;
- Limitation Act 1980;
- relevant financial, employment and health and safety legislation; and
- statutory safeguarding requirements, including **Keeping Children Safe in Education**.

The school also has regard to current guidance issued by the Department for Education, Information Commissioner's Office and other relevant regulatory bodies.

The Data (Use and Access) Act 2025 does not replace UK GDPR or the Data Protection Act 2018 but amends and builds upon the existing framework.

4. Records Management Principles

The school will ensure, as far as reasonably practicable, that records are:

Accurate – records should provide a reliable account of the information, action, decision or event they document.



Adequate and relevant – sufficient information should be recorded for the purpose for which the record is required, without collecting or retaining unnecessary information.

Clear – records should be written in a way that can be understood by an appropriate person who may need to use them in future.

Authentic – it should be possible to establish what a record relates to, who created it and, where relevant, when it was created or amended.

Secure – records must be protected against unauthorised access, alteration, loss, destruction or disclosure.

Accessible – authorised people should be able to locate and retrieve information when it is legitimately required.

Retained appropriately – records must be kept for as long as they are required, but not indefinitely without justification.

Disposed of securely – records that have reached the end of their retention period and are no longer required must be securely destroyed or anonymised unless there is a legitimate reason for continued retention.

The ICO's storage-limitation principle requires organisations to be able to justify how long personal information is retained and to review and erase or anonymise information when it is no longer required.

5. Roles and Responsibilities

Governing Board

The Governing Board is responsible for:

- ensuring appropriate records-management and data-protection arrangements are in place;
- approving this policy;
- providing appropriate oversight; and

- 
- ensuring the school has access to appropriate Data Protection Officer advice.

Headteacher

The Headteacher has overall operational responsibility for ensuring that effective records-management arrangements are implemented across the school.

This includes ensuring that:

- staff understand their responsibilities;
- appropriate systems and procedures are in place;
- records are stored and handled securely;
- the Record Retention Schedule is implemented;
- information incidents are appropriately managed; and
- appropriate advice is sought where required.

Data Protection Officer

The Data Protection Officer (DPO) provides independent advice and oversight in relation to the school's compliance with data-protection legislation.

The DPO may advise on:

- retention and disposal;
- information rights requests;
- data breaches;
- data sharing;
- privacy risks;
- records containing personal information; and
- other data-protection matters.



Designated Safeguarding Lead

The Designated Safeguarding Lead (DSL) is responsible for ensuring that safeguarding and child-protection records are created, maintained, accessed, transferred and retained in accordance with current statutory safeguarding requirements and school procedures.

School Business Manager and Administrative Staff

Staff with administrative, finance, HR or records-management responsibilities will ensure that records within their areas are managed in accordance with this policy and the Record Retention Schedule.

All Staff

Everyone who handles personal data in school has responsibility for protecting it. Current DfE guidance explicitly applies that responsibility to all staff.

Staff must:

- create accurate and appropriate records;
- use school-approved systems;
- store information securely;
- only access information they are authorised to access;
- not remove, alter or destroy records without authority;
- follow the Record Retention Schedule;
- report loss, unauthorised disclosure or other information incidents promptly; and
- seek advice where they are uncertain about how a record should be handled.



6. Creating and Maintaining Records

Records should be created where they are necessary to provide evidence of school business, decisions, actions, events or responsibilities.

Records should be:

- factual and accurate;
- created promptly;
- dated where appropriate;
- attributable to the person creating them;
- written professionally;
- sufficiently detailed to enable the matter to be understood later; and
- stored in the appropriate school system or location.

Staff should distinguish clearly between fact, professional judgement, opinion and information reported by another person.

Records should not contain unnecessary, excessive, speculative or inappropriate personal comments.

Where an error is identified, the record should be corrected in a way that preserves an appropriate audit trail where required. Records should not be altered or deleted simply because their content later becomes inconvenient or disputed.

Staff should work on the basis that records containing personal information may potentially be disclosed to the person concerned through information-rights legislation, subject to any applicable exemptions.

7. Pupil and Educational Records

The school will maintain appropriate records for each pupil.

Records may include, where relevant:

- 
- admission and identification information;
 - attendance;
 - assessment and attainment;
 - curriculum and educational information;
 - SEND and additional-needs information;
 - behaviour and pastoral information;
 - medical information required by the school;
 - communications with parents/carers;
 - reports;
 - information received from previous education settings;
 - information about support and interventions; and
 - other information necessary to educate, support or safeguard the pupil.

Pupil records must be managed securely and access restricted to those with a legitimate reason to view them.

Information should be stored within the appropriate school system rather than unnecessarily duplicated across personal folders, emails or local devices.

When a pupil leaves the school, relevant records will be transferred and/or retained in accordance with statutory requirements and the school's Record Retention Schedule.

The school will maintain sufficient evidence of significant record transfers where appropriate.

8. Safeguarding and Child Protection Records

Safeguarding records require particularly careful management because of their sensitivity and importance to children's welfare.

Safeguarding and child-protection records must:

- 
- be accurate, clear and appropriately detailed;
 - distinguish fact from opinion;
 - identify the concern or allegation;
 - record actions taken;
 - record decisions reached and the rationale for those decisions where appropriate;
 - record relevant outcomes;
 - be stored securely;
 - be accessible only to those who require access for legitimate safeguarding purposes; and
 - be retained and transferred in accordance with current statutory safeguarding requirements.

Safeguarding records must be maintained separately from the ordinary pupil educational record, whether held physically or electronically.

Transfer to another school or college

When a pupil transfers to another school or college, the DSL will ensure that the child-protection file is transferred:

- **separately from the main pupil file;**
- securely;
- as soon as practicable in accordance with current safeguarding requirements; and
- with confirmation of receipt obtained and retained where required.

The receiving DSL should be informed of information necessary to enable appropriate support to be put in place.

The school will not routinely create or retain unnecessary duplicate copies of transferred safeguarding case files. Any records retained following transfer will be those required by the Record Retention Schedule or necessary to evidence the transfer or meet another legitimate requirement.

Current DfE retention guidance states that child-protection files should be passed to a child's new school separately from the main pupil file.



Allegations relating to staff

Records relating to allegations against staff will be managed in accordance with current **Keeping Children Safe in Education**, the school's safeguarding procedures and the Record Retention Schedule.

KCSIE 2026 distinguishes between allegations found to be malicious or false and other outcomes. Details of allegations found following investigation to be malicious or false should normally be removed from personnel records unless the individual consents to their retention. Records of other allegations require an appropriate summary, outcome and record of actions and decisions.

Low-level concerns will be managed in accordance with KCSIE and the school's Low-Level Concerns procedures.

9. SEND and Additional-Needs Records

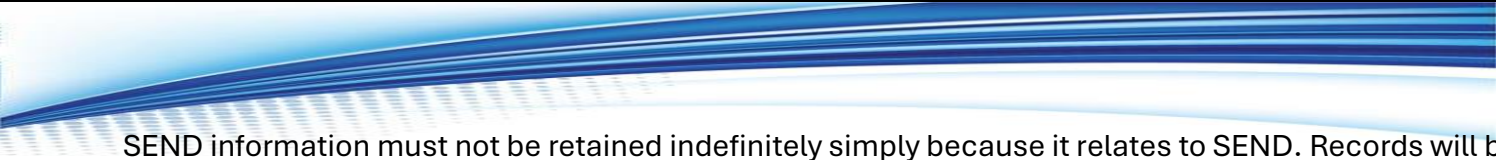
Records relating to SEND and additional needs must be accurate, relevant and proportionate.

The school will distinguish between:

- statutory or significant records requiring longer-term retention; and
- routine working documents or duplicated information that does not require equivalent retention.

Relevant records may include:

- Education, Health and Care Plan documentation;
- statutory assessment information;
- professional reports;
- records of significant provision and support;
- review documentation;
- correspondence with external agencies; and
- other information necessary to demonstrate how the school has identified and met a pupil's needs.



SEND information must not be retained indefinitely simply because it relates to SEND. Records will be retained in accordance with their purpose and the Record Retention Schedule.

10. Storage and Security

Records must be stored in a manner appropriate to their sensitivity and importance.

Paper records

Confidential paper records should:

- be stored securely;
- be protected from unauthorised access;
- not be left unattended in public or insecure areas;
- only be removed from school where authorised and necessary; and
- be transported securely where removal is necessary.

Electronic records

Electronic records must be stored using school-approved systems and must be protected through appropriate technical and organisational security measures.

Staff must follow the school's requirements relating to:

- passwords and authentication;
- access permissions;
- devices;
- remote working;
- cloud services;

- 
- email;
 - cyber security;
 - removable media; and
 - reporting security incidents.

Personal accounts, personal cloud-storage services and unauthorised devices or applications must not be used to store school records.

Detailed requirements are set out in the school's **Accountable Use of ICT, Online Services and Digital Technology Policy**.

11. Email, Messaging and Digital Communications

Email and other electronic communications may constitute school records.

Where a communication provides significant evidence of:

- a decision;
- an agreement;
- an action;
- a safeguarding matter;
- a complaint;
- professional advice;
- a contractual matter; or
- another significant school activity,

it should be retained in the appropriate school record or system where necessary.

Staff should not use their email inbox as the sole long-term repository for important school records.



Routine emails and messages with no continuing business, legal, safeguarding or evidential value do not need to be retained indefinitely.

The same retention principles apply to electronic information regardless of whether it is held in email, SharePoint, an MIS, CPOMS, another cloud service or an archived system.

12. Information Mapping and Records of Processing

The school will maintain appropriate documentation of the personal information it processes.

This should enable the school to understand, where appropriate:

- what information it holds;
- why it holds it;
- whose information it is;
- where it is stored;
- who has access to it;
- who it is shared with;
- the lawful basis for processing;
- how long it should be retained; and
- how it will ultimately be disposed of.

The school's information asset register, record of processing activities and Record Retention Schedule may be used together to provide this oversight.

13. Access to Records and Information Rights

Access to school records is restricted according to role and legitimate need.



Employees must not access records merely because the system allows them to do so.

Requests for access to information may arise under:

- UK GDPR/Data Protection Act 2018;
- Freedom of Information Act 2000;
- Environmental Information Regulations 2004;
- education legislation; or
- other legal processes.

Such requests must be referred promptly to the appropriate person and handled in accordance with the school's relevant procedures.

Good record keeping and appropriate retention arrangements make it easier for schools to respond properly to subject access requests.

Staff must not delete, alter or destroy information because a request for access, complaint, investigation, legal claim or other relevant process has been made or is reasonably anticipated.

14. Sharing Records

Information will only be shared where there is a lawful and legitimate reason to do so.

Before sharing information, staff should consider:

- whether sharing is necessary;
- whether the recipient is appropriate;
- what information is actually required;
- whether the information can be shared securely; and
- whether any particular safeguarding or confidentiality requirements apply.



Data protection law does **not** prevent appropriate information sharing for safeguarding purposes.

Where there is uncertainty, advice should be sought from the DSL, DPO or another appropriate senior leader according to the nature of the information.

15. Transfer of Records

Records transferred within or outside the school must be handled securely.

The method of transfer should reflect the sensitivity of the information.

Where appropriate, the school will:

- verify the intended recipient;
- use an approved secure transfer method;
- maintain appropriate records of transfer;
- obtain confirmation of receipt; and
- avoid retaining unnecessary duplicate copies.

Where records are transferred to another organisation, responsibility for retention should be clear.

Particular requirements for safeguarding records are set out in Section 8.

16. Record Retention Schedule

The school's **Record Retention Schedule** forms part of its records-management arrangements and must be followed by all staff.

The schedule identifies:

- 
- categories of records;
 - standard retention periods;
 - the event from which the retention period runs where appropriate; and
 - the action to be taken at the end of the retention period.

Retention periods may be based on:

- statutory requirements;
- safeguarding requirements;
- regulatory guidance;
- limitation periods;
- financial or audit requirements;
- contractual requirements;
- operational need; and
- recognised records-management practice.

The UK GDPR does not establish one universal period for retaining personal data. The school must be able to justify its retention periods according to the purpose for which information is held.

Exceptions to standard retention periods

A record must **not** be destroyed simply because its standard retention period has expired where it remains relevant to:

- an ongoing safeguarding matter;
- litigation or a potential legal claim;
- a complaint;
- an investigation;
- an insurance matter;
- an audit;

- 
- an information-rights request;
 - a police or regulatory matter; or
 - another legitimate reason requiring continued retention.

In these circumstances, destruction should be suspended until it is confirmed that the record may lawfully be disposed of.

Where there is uncertainty about the appropriate retention period, **the record must not be destroyed until advice has been obtained from the Data Protection Officer and, where relevant, the Designated Safeguarding Lead or other appropriate professional adviser.**

17. Reviewing and Weeding Records

Records should be reviewed periodically to ensure that information is not retained unnecessarily.

The school will make appropriate arrangements for regular review and disposal of records that have reached the end of their retention period.

Departments and record owners should not accumulate records indefinitely.

Review may include:

- deleting duplicate copies;
- removing superseded working documents;
- deleting routine correspondence that no longer has value;
- identifying records that have reached their disposal date;
- anonymising information where identification is no longer required; and
- identifying records that should be retained for longer because of a legitimate reason.

ICO guidance specifically recommends periodic weeding to prevent information becoming excessive, inaccurate or unnecessarily retained.



18. Archives, Backups and Deleted Accounts

Moving information from an active system into an **archive does not itself satisfy the requirement to delete information** when its retention period expires.

Retention and disposal requirements apply to electronic and archived records as well as paper records.

The school will work with relevant system providers and IT support to ensure that, as far as reasonably practicable:

- archived information is subject to appropriate retention arrangements;
- records associated with former users are appropriately reviewed;
- information is not retained indefinitely merely because a system permits it;
- backup arrangements are appropriate and secure; and
- deleted information is dealt with in accordance with system capabilities, contractual arrangements and data-protection requirements.

Backups are primarily maintained for system recovery and business continuity and should not routinely be used as permanent archives.

19. Secure Disposal and Destruction

Records that have reached the end of their retention period and are no longer required will be securely disposed of.

Paper records

Confidential paper records must be destroyed through an approved secure method, such as confidential-waste destruction or cross-cut shredding as appropriate.



They must not be placed in ordinary waste or recycling where personal, confidential or sensitive information could be reconstructed or accessed.

Electronic records

Electronic records must be securely deleted using an appropriate method.

Deleting a shortcut, moving a file to a recycle bin or removing information from an individual's view may not constitute secure deletion.

Where devices or storage media are being reused, transferred or disposed of, school information must be securely erased in accordance with the school's ICT and asset-disposal arrangements.

Where destruction is carried out by an external provider, appropriate assurances and contractual arrangements must be in place.

Records of destruction should be retained where this is appropriate because of the nature or sensitivity of the records concerned.

20. Records of Historical Value

Some records may have enduring historical or archival value.

Where the school considers that a record should be retained permanently for legitimate historical or archival purposes, this should be identified within its records-management arrangements.

Any continued retention of personal information for archiving purposes must comply with applicable data-protection requirements and appropriate safeguards.

Records must not simply be kept permanently because they are interesting or *might* be useful one day.



21. Loss, Damage or Unauthorised Disclosure of Records

Any actual or suspected:

- loss of records;
- unauthorised access;
- accidental disclosure;
- inappropriate alteration;
- destruction;
- theft;
- cyber incident affecting records; or
- other personal-data breach

must be reported **immediately** through the school's agreed reporting procedures.

Staff must not attempt to conceal an information incident.

The Headteacher, DPO, DSL and/or IT support will be involved according to the nature of the incident.

Where required, the school will assess whether the incident must be reported to the Information Commissioner's Office, affected individuals, police, Local Authority or another relevant body.

22. Records Relating to Staff Who Leave

When an employee leaves the school:

- school records in their possession must be returned;
- access to school systems will be removed in accordance with agreed procedures;
- important business records held within their accounts or folders must be transferred to an appropriate location;

- 
- school information must not be retained on personal devices or personal accounts; and
 - relevant employment records will be retained in accordance with the Record Retention Schedule.

The school may retain or access business records within a former employee's school account where necessary and lawful for legitimate school purposes.

23. Training and Awareness

Staff will receive appropriate information and training about records management and data protection relevant to their roles.

This will include, as appropriate:

- secure handling of information;
- record creation;
- retention and disposal;
- information sharing;
- cyber security;
- information rights;
- safeguarding records; and
- reporting information incidents.

Staff with specialist responsibilities may receive additional training.

24. Related Policies and Documents

This policy should be read alongside the school's:

- Record Retention Schedule;
- Data Protection Policy and Privacy Notices;

- 
- Freedom of Information Publication Scheme and Guide to Information;
 - Child Protection and Safeguarding Policy;
 - Low-Level Concerns Policy;
 - Allegations Against Staff procedures;
 - SEND Policy;
 - Accountable Use of ICT, Online Services and Digital Technology Policy;
 - Acceptable Use of Mobile Phones, Cameras and Image-Recording Devices Policy;
 - Online Safety Policy;
 - CCTV arrangements/privacy information;
 - Complaints Policy;
 - Health and Safety Policy;
 - Staff Code of Conduct;
 - Finance Policy and financial procedures; and
 - relevant HR and employment procedures.

25. Monitoring and Review

The school will monitor its records-management arrangements and take action where:

- records are being retained unnecessarily;
- records cannot readily be located;
- inappropriate duplication occurs;
- systems or working practices change;
- information incidents identify weaknesses;
- legislation or guidance changes; or
- the Record Retention Schedule requires amendment.



The school will periodically review the personal information it holds and securely erase or anonymise information that is no longer required. This reflects the current ICO storage-limitation principle.

This policy will be formally reviewed every two years, or sooner where necessary.

Templars Primary School
Record Retention Schedule

Policy Owner: Headteacher

Operational Leads: School Business Manager / Data Protection Lead

Professional Advice: Data Protection Officer

Approval: Governing Board

Date Reviewed: Summer 2026

Review Cycle: Annual

Next Review Due: Summer 2027, or sooner where legislation, statutory guidance or relevant Local Authority advice changes

1. Purpose

This Record Retention Schedule forms part of Templars Primary School's records-management arrangements and should be read alongside the school's **Records Management Policy**.

It sets out:

- how long categories of school records should normally be retained;
- the basis for the retention period;
- what should happen when the retention period expires; and
- where records require review rather than automatic destruction.

The schedule applies to records in **all formats and locations**, including:

- paper files;
- the school's Management Information System (MIS);
- CPOMS and other safeguarding systems;
- SharePoint and approved cloud services;
- email and electronic communications;

- 
- personnel systems and files;
 - photographs, video and audio;
 - CCTV;
 - databases and online forms;
 - archived records; and
 - records held on behalf of the school by data processors.

The retention period applies to the **record and information**, not merely the particular system in which it is stored.

Archiving a record does not constitute disposal.

2. Status of Retention Periods

To avoid confusing legal requirements with locally determined retention periods, this schedule uses the following classifications.

STATUTORY / LEGAL

A retention period derives directly from legislation or a legal requirement identified in current authoritative guidance.

DfE / KCSIE

The period or minimum expectation is specified in current Department for Education guidance or *Keeping Children Safe in Education*.

OTHER NATIONAL REQUIREMENT

The period derives from another authoritative government or regulator source, such as the Home Office, DBS, HMRC or HSE.

LOCAL BUSINESS PERIOD

There is no nationally prescribed period applying specifically to that record. Templars has selected a proportionate period based on:

- the purpose for which the information is held;
- operational need;
- limitation and litigation risk;
- safeguarding or evidential need;
- financial or audit requirements; and
- the UK GDPR storage-limitation principle.

REVIEW



The record must be reviewed before destruction because circumstances may justify continued retention.

A **LOCAL BUSINESS PERIOD** is not represented as a statutory retention requirement and should be kept under review with the school's Data Protection Officer.

3. General Rules Applying to Every Record

Personal data must not be kept longer than necessary.

Before retaining information, the school should be able to identify:

- why the information is held;
- the lawful basis for processing it;
- whether there is a specific legal retention requirement;
- whether another organisation is the appropriate long-term record holder;
- whether the record is still required once it has been transferred elsewhere; and
- how the record will ultimately be destroyed, transferred or archived.

The school will review the personal information it holds at least annually.

Where the same information exists in several systems or locations, unnecessary duplicates should not be retained merely because the principal record remains subject to retention.

4. Suspension of Destruction — Legal and Safeguarding Hold

No record must be destroyed merely because its normal retention period has expired where it is, or may reasonably become, relevant to:

- an ongoing safeguarding matter;
- an allegation against an adult;
- litigation or a reasonably anticipated legal claim;
- a complaint;
- an insurance claim;
- a disciplinary, grievance or employment process;
- an investigation;
- a police, LADO, regulatory or Local Authority matter;
- an audit;

- an information-rights request, including a Subject Access Request or Freedom of Information request; or
- another legitimate process requiring preservation of evidence.

Where one of these circumstances applies, normal destruction will be **suspended** until the matter and any relevant review, appeal or limitation period has concluded and the appropriate person confirms that destruction may resume.

Staff must not alter, erase, destroy, conceal or otherwise dispose of records with the intention of preventing disclosure following a Freedom of Information request or other lawful information request.

Where there is uncertainty, the record must not be destroyed until advice has been obtained from the DPO and, where applicable, the DSL, HR adviser, insurer or legal adviser.

PART A — PUPILS AND SAFEGUARDING

5. Main Pupil Records

Record	Retention Period	Basis	End Action
Primary school pupil record	Until pupil leaves Templars	DfE / pupil information requirements	Transfer securely to receiving school
MIS pupil data after pupil leaves	2 terms after leaving, where required for school census purposes	DfE	Delete/anonymise information no longer otherwise required
Curricular record	At least 1 year	DfE / education records requirements	Secure destruction
Significant assessment and attainment information forming part of pupil record	Until transfer with pupil record	DfE / operational	Transfer
Routine teacher assessment and tracking working documents	Current academic year + 1 year	LOCAL BUSINESS PERIOD	Secure destruction unless still required
Pupil work retained by school	While educationally required	LOCAL BUSINESS PERIOD	Return, anonymise or securely dispose

Record	Retention Period	Basis	End Action
Significant behaviour/pastoral information forming part of pupil record	Until pupil leaves / transfer as appropriate	LOCAL BUSINESS PERIOD based on continuing educational need	Transfer relevant record
Routine minor behaviour records with no continuing significance	Current academic year + 1 year	LOCAL BUSINESS PERIOD	Secure destruction

Important distinction

The **primary pupil record is not routinely retained by Templars until the child's 25th birthday**. On leaving a primary school it transfers to the next school. Information still required for census purposes may remain on the MIS for two terms.

6. Safeguarding and Child Protection

Record	Retention Period	Basis	End Action
Child protection file	Until child's 25th birthday	DfE safeguarding retention requirement	Secure destruction at final retention point
Child protection file relating to child sexual abuse	Until child's 75th birthday	DfE / IICSA	Secure destruction at final retention point
Safeguarding chronology, referrals, strategy information, professional correspondence, decisions and outcomes	Same period as safeguarding file	DfE / KCSIE	Retain as part of safeguarding file
Record confirming transfer of child-protection file	Retain as evidence of secure transfer for an appropriate period determined with DPO/DSL	LOCAL BUSINESS / evidential	Review then securely destroy

Transfer of safeguarding files

When a pupil moves school or college, the DSL or deputy must ensure the child-protection file is:

- transferred **separately from the main pupil file**;

- transferred securely;
- transferred as soon as possible and within the timescales required by KCSIE;
- accompanied where necessary by advance information to enable the receiving school to manage risk; and
- acknowledged by the receiving school, with confirmation of receipt obtained.

The school must not keep unnecessary duplicate safeguarding case files simply because information has transferred. The DSL and DPO should determine what limited evidence of transfer Templates needs to retain.

7. Allegations Against Staff

Allegations that may meet the harm threshold

Record	Retention Period	Basis	End Action
Substantiated allegation	At least until accused reaches normal pension age , or 10 years from date of allegation , whichever is longer	KCSIE 2026	Secure destruction following review
Unfounded allegation	Same period	KCSIE 2026	Secure destruction following review
Unsubstantiated allegation	Same period	KCSIE 2026	Secure destruction following review
False or malicious allegation	Remove from personnel record unless the individual consents to retention or another lawful reason applies	KCSIE 2026	Remove securely following safeguarding/HR advice

For allegations other than false or malicious allegations, the retained record should contain the information required by KCSIE, including:

- a clear summary of the allegation;
- how it was followed up and resolved;
- action taken;
- decisions reached;
- the outcome; and
- the required statement regarding future references.

8. Low-Level Concerns About Adults

Record	Retention Period	Basis	End Action
Low-level concern record	At least until the individual leaves employment	KCSIE 2026 recommendation	REVIEW with Headteacher/DSL/DPO before destruction

Pattern/group of concerns which develops into misconduct or meets harm threshold	Follow relevant disciplinary/allegations retention requirement	KCSIE 2026	Retain accordingly
--	--	------------	--------------------

There is **no fixed statutory number of years** for low-level concerns.

KCSIE states that schools may determine their own period, but recommends retaining such records at least until the individual leaves employment.

The school will consider longer retention where there is a continuing safeguarding, pattern, disciplinary or evidential need.

9. SEND and Additional Needs

There is **no universal statutory retention period simply because a record relates to SEND.**

Retention will therefore depend on the nature and purpose of the particular record.

Record	Retention Period	Basis	End Action
EHCP/statutory assessment material needed to support pupil	While pupil attends and information remains relevant; transfer appropriate record	LOCAL BUSINESS / continuing educational need	Transfer/review
Significant professional reports	While relevant to pupil's education and provision; transfer where required	LOCAL BUSINESS	Transfer/review
Significant review and provision records	While pupil attends and required to evidence provision; relevant information transferred	LOCAL BUSINESS	Transfer/review
Routine intervention working notes	Current academic year + 1 year unless required longer to evidence provision/progress	LOCAL BUSINESS PERIOD	Secure destruction

Record	Retention Period	Basis	End Action
Screening records	While relevant to continuing education/support	LOCAL BUSINESS PERIOD	Transfer relevant outcome or destroy
Provision maps	Current academic year + 3 years	LOCAL BUSINESS PERIOD	Secure destruction or anonymise for strategic analysis

If an SEND document is also a **safeguarding record**, the safeguarding retention requirement takes precedence. Where information forms part of an ongoing complaint, tribunal, statutory assessment dispute or legal claim, destruction must be suspended.

10. Admissions and Attendance

Record	Retention Period	Basis	End Action
Admission register entries	6 years from date of admission/entry	STATUTORY / DfE	Secure destruction
Attendance register entries	6 years from date of entry	STATUTORY / DfE	Secure destruction
Successful admission application material	Until relevant information incorporated into pupil record and no longer separately required	LOCAL BUSINESS	Secure destruction of duplicate material
Unsuccessful admission application	Academic year + 1 year, unless appeal/complaint is continuing	LOCAL BUSINESS PERIOD	Secure destruction
Admission appeal	6 years after conclusion	LOCAL BUSINESS PERIOD based on limitation/evidential need	Secure destruction
Proof of address/eligibility evidence	Until admission process and challenge period conclude unless otherwise required	LOCAL BUSINESS	Secure destruction
Routine attendance correspondence	2 years after matter concludes	LOCAL BUSINESS PERIOD	Secure destruction

Record	Retention Period	Basis	End Action
Attendance material forming part of safeguarding intervention	Safeguarding retention period	DfE/KCSIE	Retain in safeguarding file

11. Educational Visits, Trips and Activities

Record	Retention Period	Basis	End Action
Educational visit record	10 years from date of visit	DfE	Secure destruction
Visit involving an incident	10-year visit record plus relevant incident/permission material retained in pupil record as required	DfE	Review according to pupil/incident record
Visit risk assessment	10 years where part of formal visit record	LOCAL BUSINESS aligned with DfE visit period	Secure destruction
Routine club/activity register	Current academic year + 3 years	LOCAL BUSINESS PERIOD	Secure destruction

PART B — GOVERNANCE AND SCHOOL MANAGEMENT

12. Governance

Record	Retention Period	Basis	End Action
Governing Board meeting records	10 years from date of meeting	DfE	Secure destruction or archival review
Confidential Governing Board records	Same period as corresponding meeting record	DfE / LOCAL security control	Secure destruction

Record	Retention Period	Basis	End Action
Annual governors' report where applicable	10 years	DfE	Secure destruction
Instrument of Government	Life of instrument / permanent historical copy	LOCAL ARCHIVAL / governance requirement	Archive
Terms of reference / governance structure	Current + previous 6 years	LOCAL BUSINESS PERIOD	Review
Governor declarations of interests	While current + 6 years after governor leaves	LOCAL BUSINESS PERIOD	Secure destruction
Governor training record	Term of office + 6 years	LOCAL BUSINESS PERIOD	Secure destruction

Records of genuine historical significance may be selected for permanent preservation.
Permanent archive should be a deliberate decision, not the default alternative to destruction.

13. Strategic, Policy and Curriculum Records

Record	Retention Period	Basis	End Action
School Improvement/Development Plan	Current + 6 years	LOCAL BUSINESS PERIOD	Review for archive
SEF/self-evaluation documents	Current + 6 years	LOCAL BUSINESS PERIOD	Review
Ofsted inspection reports	Permanent/public record	ARCHIVAL	Archive/reference
Major external review reports	10 years or permanent where historically significant	LOCAL BUSINESS/ARCHIVAL	Review
School policies	Current version + previous version for 6 years	LOCAL BUSINESS PERIOD	Secure destruction/archive significant policies
Curriculum frameworks/policies	Current + 6 years	LOCAL BUSINESS PERIOD	Review

Record	Retention Period	Basis	End Action
Routine lesson planning/schemes	Current + 1 year after superseded unless required longer	LOCAL BUSINESS PERIOD	Secure destruction
Timetables	Current + 1 year	LOCAL BUSINESS PERIOD	Secure destruction
Strategic SLT records	6 years	LOCAL BUSINESS PERIOD	Review
Routine operational meeting notes	3 years	LOCAL BUSINESS PERIOD	Secure destruction

A significant decision should be retained within the appropriate formal record rather than relying solely on transient meeting notes or email.

PART C — STAFF AND RECRUITMENT

14. Personnel Records

Record	Retention Period	Basis	End Action
Personnel file	6 years after termination of employment	DfE	Secure destruction, subject to specific exceptions
Successful recruitment record	Necessary information incorporated into personnel file; recruitment evidence retained within applicable personnel period	DfE / LOCAL	Secure destruction
Unsuccessful applicant records	6 months after process concludes; up to 12 months where a specific equality/recruitment reason is documented	LOCAL BUSINESS PERIOD	Secure destruction
Interview notes – unsuccessful applicant	Same as unsuccessful recruitment record	LOCAL BUSINESS	Secure destruction

Record	Retention Period	Basis	End Action
Disciplinary records	In accordance with outcome/HR policy and personnel period	LOCAL BUSINESS / HR	Secure destruction subject to safeguarding exceptions
Grievance records	Employment + 6 years	LOCAL BUSINESS PERIOD	Secure destruction
Appraisal/performance records	Current cycle + previous cycles where required; normally no longer than employment + 6 years	LOCAL BUSINESS / DfE personnel framework	Secure destruction
Emergency contact information	While employed and operationally necessary	LOCAL BUSINESS	Delete promptly after leaving
Specific statutory or safeguarding records override the general six-year personnel-file period.			

15. Recruitment Checks

Record	Retention Period	Basis	End Action
DBS certificate copy	Where there is a valid reason to retain a copy: no longer than 6 months	KCSIE / DBS	Secure destruction
Record that DBS/vetting check took place and recruitment decision	Retain appropriate record/SCR while required	KCSIE	Follow personnel/SCR rules
Single Central Record entry	While individual works at school	KCSIE 2026	Remove once individual no longer works at school
Right-to-work evidence	Duration of employment plus 2 years	Home Office	Secure destruction
DBS identity-validation record/documents	Minimum 2 years where required by current DBS identity-checking rules	DBS	Secure destruction after minimum period when no longer needed

Record	Retention Period	Basis	End Action
Qualifications/identity evidence for successful candidate	Personnel file retention where necessary	KCSIE/DfE	Secure destruction at applicable end point
Safer-recruitment decision records	Personnel/recruitment period as applicable	KCSIE / LOCAL	Secure destruction

The six-month DBS certificate period is **not** the same as the retention period for evidence that appropriate vetting took place.

16. Payroll and Employment Finance

Record	Retention Period	Basis	End Action
PAYE/payroll records	3 years from end of tax year to which they relate	DfE/HMRC	Secure destruction
Statutory maternity pay records	3 years after end of tax year in which maternity-pay period ends	STATUTORY / DfE	Secure destruction
Retirement benefit records	Minimum 6 years from end of year in which relevant accounts were signed	DfE	Secure destruction subject to pension-provider requirements
Timesheets supporting payroll	6 years from relevant financial year end	LOCAL BUSINESS / financial evidence	Secure destruction
Staff expenses	6 years from relevant financial year end	LOCAL BUSINESS / financial evidence	Secure destruction

Where payroll/pension records are held as the authoritative record by Coventry City Council or another provider, Templars should retain only the duplicate information it genuinely requires.

17. Staff Health and Occupational Records

Record	Retention Period	Basis	End Action
Health surveillance records	40 years	DfE/HSE/COSHH	Secure destruction
Exposure monitoring to hazardous substances,	5 years unless a longer health-surveillance requirement applies	DfE/HSE	Secure destruction

Record	Retention Period	Basis	End Action
including asbestos where applicable			
Other staff health records covered by DfE retention guidance	While worker is employed at school	DfE	Secure destruction when no longer required, subject to HR/legal need
Routine sickness absence administration	While required for employment management; review on termination	LOCAL BUSINESS / HR	Secure destruction when no longer justified
Occupational Health reports held by school	Retain only as long as required for employment/adjustment/legal purpose	LOCAL BUSINESS / special-category data	REVIEW before destruction
Health records are special-category personal data. The school should avoid retaining detailed medical information where a less intrusive record of an adjustment or management decision is sufficient.			

PART D — HEALTH, SAFETY AND PREMISES

18. Health and Safety

Record	Retention Period	Basis	End Action
Accident record	3 years from date of accident	DfE / statutory basis	Secure destruction unless continuing claim/need
Pupil accident record	Retain appropriately in pupil record	DfE	Transfer/manage with pupil record
Accessibility Plan	Life of plan + 6 years	DfE	Secure destruction
Fire risk assessment	Life of assessment + 6 years	DfE	Secure destruction
General significant risk assessment	Life of assessment + 6 years	LOCAL BUSINESS aligned with limitation risk	Secure destruction
Fire log book	6 years after final entry	LOCAL BUSINESS PERIOD	Secure destruction

Record	Retention Period	Basis	End Action
Significant incident investigation	6 years after closure or longer where legal/insurance hold applies	LOCAL BUSINESS	Review
RIDDOR/other statutory incident documentation	At least applicable statutory period; align with H&S adviser/insurer	OTHER NATIONAL REQUIREMENT	Secure destruction following review

19. Medical Records Relating to Pupils

There is no single national retention period applying to every school medical record.

Record	Retention Period	Basis	End Action
Current Individual Healthcare Plan	While current and required	LOCAL BUSINESS	Replace/review when superseded
Superseded healthcare plan	While necessary to evidence historic provision/incident; normally current + 1 year unless a longer reason exists	LOCAL BUSINESS PERIOD	Secure destruction
Medication administration record	Retain while necessary to evidence administration and manage any incident/claim; normally pupil attendance + appropriate review period	LOCAL BUSINESS – DPO/insurer confirmation advised	REVIEW
Allergy/dietary information	While current and necessary	LOCAL BUSINESS	Delete superseded duplicates promptly
Significant medical incident	Follow accident/pupil record/legal-hold requirements	DfE / LOCAL	Review

The school should avoid applying a blanket **DOB +25** period to all medication records without a documented reason.

20. Premises, Property and Assets

Record	Retention Period	Basis	End Action
Maintenance records	6 years from financial year end	DfE	Secure destruction



Record	Retention Period	Basis	End Action
Title deeds	12 years from end of deed	DfE / Limitation Act	Review/archive
Asset register	Life of asset + 6 years after disposal	LOCAL BUSINESS	Secure destruction
Asset disposal/write-off records	6 years from financial year end	LOCAL BUSINESS / finance	Secure destruction
Building plans	Life of building/premises and while operationally required	LOCAL BUSINESS / ARCHIVAL	Review/archive
Contractor records	Contract + 6 years unless executed as deed or H&S reason requires longer	LOCAL/limitation	Secure destruction
School vehicle records	6 years from disposal	DfE	Secure destruction

PART E — FINANCE

21. Financial Records

Record	Retention Period	Basis	End Action
Contracts	6 years from last payment	DfE / Limitation Act	Secure destruction
Contract executed as deed	Normally 12 years following applicable contractual end/claim period	LEGAL / Limitation	Review
Debtor records	6 years from financial year end	DfE	Secure destruction
VAT records	6 years from financial year end	DfE/HMRC	Secure destruction
Invoices	6 years from financial year end	LOCAL BUSINESS aligned with VAT/audit	Secure destruction

Record	Retention Period	Basis	End Action
Purchase orders	6 years from financial year end	LOCAL BUSINESS	Secure destruction
Bank statements	6 years from financial year end	LOCAL BUSINESS	Secure destruction
Annual accounts	6 years from financial year end; consider archival copy	LOCAL BUSINESS	Review
Budget-monitoring records	6 years from financial year end	LOCAL BUSINESS	Secure destruction
Petty cash records	6 years from financial year end	LOCAL BUSINESS	Secure destruction
School fund records	6 years from financial year end	LOCAL BUSINESS	Secure destruction

Where Coventry financial regulations specify a longer period, the longer applicable requirement should be followed.

PART F — INFORMATION GOVERNANCE AND DIGITAL RECORDS

22. CCTV

There is **no universal statutory 30-day CCTV retention rule**.

Templars adopts the following period based on its security and safeguarding purpose:

Record	Retention Period	Basis	End Action
Routine CCTV footage	Normally 30 days	LOCAL BUSINESS PERIOD	Automatic secure overwrite/deletion
CCTV preserved for incident, safeguarding matter, complaint, crime, insurance or legal matter	Until that purpose and any appeal/claim/investigation has concluded	LOCAL BUSINESS / LEGAL HOLD	Secure destruction following review

The stated period must match the school's actual CCTV system configuration and privacy information.

23. Photographs, Video and Audio

Record	Retention Period	Basis	End Action
Routine curriculum images/video	Until educational purpose is complete	LOCAL BUSINESS	Secure deletion
Publicity/website images	While current and authorised for stated purpose	LOCAL BUSINESS	Periodic review/deletion
Pupil progress images forming part of formal educational record	Follow pupil-record retention requirement	DfE / LOCAL	Transfer/dispose accordingly
Historic school photographs intentionally selected for archive	Permanent where archival justification recorded	ARCHIVAL	Archive securely
Audio/video recording of meeting	Delete once agreed written record has been produced unless recording itself remains necessary	LOCAL BUSINESS	Secure deletion
Training/webinar recordings involving identifiable staff/pupils	Until training/operational purpose concludes	LOCAL BUSINESS	Secure deletion

24. Email, Teams, SharePoint and Other Digital Communications

A communication is retained according to **what it records**, not according to the fact that it is an email or message.

Record	Retention	Basis	End Action
Routine email/messages with no ongoing value	Delete when no longer operationally required	LOCAL BUSINESS	Delete
Significant decision/agreement	File in appropriate formal record and follow that record's retention period	Records Management Policy	Delete unnecessary duplicate email
Safeguarding communication	Safeguarding retention period	DfE/KCSIE	Retain within safeguarding record
HR communication	Relevant HR/personnel period	DfE/LOCAL	File appropriately

Record	Retention	Basis	End Action
Complaint correspondence	Complaint period	LOCAL BUSINESS	File appropriately
Finance correspondence	Relevant finance period	DfE/LOCAL	File appropriately
Staff inboxes and individual OneDrive accounts must not be treated as permanent archives.			

25. Data Protection Records

Record	Retention Period	Basis	End Action
Record of Processing Activities	Current plus previous versions necessary to evidence compliance	UK GDPR accountability / LOCAL	Review
Data Protection Impact Assessment	Life of processing activity + 6 years	LOCAL BUSINESS / accountability	Secure destruction
Data-sharing agreement	Life of agreement + 6 years	LOCAL BUSINESS / contractual	Secure destruction
Data processor contract	Contract + 6 years	LOCAL BUSINESS / limitation	Secure destruction
Personal-data breach record	6 years after closure	LOCAL BUSINESS PERIOD to evidence accountability	Secure destruction
Information Asset Register	Current + superseded versions only while necessary to evidence compliance	LOCAL BUSINESS	Review

26. Subject Access Requests

There is **no fixed UK GDPR retention period** for the administrative file relating to a Subject Access Request.

Templars adopts:

Record	Retention Period	Basis	End Action
SAR request, correspondence, search/decision log and response evidence	2 years after completion	LOCAL BUSINESS PERIOD	Secure destruction

Record	Retention Period	Basis	End Action
Underlying records disclosed/withheld	Follow their own substantive retention period	Existing schedule	Do not destroy early solely because SAR complete

Where a dispute, ICO complaint or legal claim remains possible or ongoing, retain until resolved.

27. Freedom of Information Requests

Record	Retention Period	Basis	End Action
FOI request and response administration	3 years after final closure	LOCAL BUSINESS PERIOD	Secure destruction
Information withheld/subject to review or ICO complaint	Preserve until internal review/ICO/appeal process is conclusively complete, then apply substantive retention rule	FOIA/ICO	Review

Information scheduled for destruction must not be deliberately destroyed to prevent its disclosure following receipt of an FOI request.

28. Cyber-Security and System Records

Record	Retention Period	Basis	End Action
Significant cyber-security incident file	6 years after closure	LOCAL BUSINESS PERIOD	Secure destruction
Routine technical/security logs	Period defined according to documented security purpose; normally measured in months, not indefinitely	LOCAL BUSINESS / UK GDPR	Automated deletion
Former staff user account	Disable promptly on leaving; extract legitimate records; delete account according to approved IT offboarding procedure	Cyber/data protection	Delete

Record	Retention Period	Basis	End Action
Backups	According to documented backup cycle	Cyber/business continuity	Automatic overwrite

Backups must not be used as a means of retaining records indefinitely after their substantive retention period has expired.

PART G — COMPLAINTS, VISITORS AND COMMUNITY

29. Complaints

There is no single statutory six-year period governing every school complaint.

Templars adopts:

Record	Retention Period	Basis	End Action
Routine school complaint	6 years after final resolution	LOCAL BUSINESS PERIOD based on evidential/limitation need	Secure destruction
Complaint involving safeguarding	Safeguarding period where record forms part of safeguarding file	DfE/KCSIE	Retain accordingly
Complaint involving litigation/potential litigation	Suspend destruction until matter and relevant limitation period conclude	LEGAL HOLD	Review
Vexatious/persistent communication management record	6 years after final conclusion where required to evidence decisions	LOCAL BUSINESS	Review

30. Visitors and Site Security

There is **no nationally prescribed universal retention period for routine school visitor logs**.

Templars adopts:

Record	Retention Period	Basis	End Action
Routine visitor sign-in records	Current academic year + 1 year	LOCAL BUSINESS PERIOD based on safeguarding/security need	Secure destruction

Record	Retention Period	Basis	End Action
Contractor visitor/sign-in records	Current year + 3 years	LOCAL BUSINESS PERIOD	Secure destruction
Visitor record relevant to safeguarding/security incident	Follow related safeguarding/incident period	DfE/LOCAL	Retain within incident record
Formal site-access restriction/bar	Duration of restriction + 6 years after conclusion	LOCAL BUSINESS PERIOD	Review

31. Family Support, Early Help and Pastoral Records

Retention depends on the substance of the record rather than the job title of the person creating it.

Record	Retention Period	Basis	End Action
Early Help/family-support information forming part of child-protection file	Safeguarding retention period	DfE/KCSIE	Retain accordingly
Significant pastoral record forming part of pupil record	Pupil-record period	DfE/LOCAL	Transfer
Routine family-support working notes not required as safeguarding/pupil record	Case closure + 3 years	LOCAL BUSINESS PERIOD	Secure destruction
External-agency referral evidence	While relevant to continuing support; if safeguarding, safeguarding period	LOCAL BUSINESS / safeguarding	Review
Family-support group register	Current year + 3 years	LOCAL BUSINESS PERIOD	Secure destruction

32. Catering and Free School Meals

Record	Retention Period	Basis	End Action
Routine meal register	Current academic year + 3 years unless financial/audit requirement requires longer	LOCAL BUSINESS PERIOD	Secure destruction

Record	Retention Period	Basis	End Action
Catering finance records	6 years from financial year end	LOCAL BUSINESS aligned with finance requirements	Secure destruction
Current allergy/dietary information	While necessary and current	LOCAL BUSINESS	Delete superseded duplicates
School-held FSM eligibility evidence	Retain only while required for entitlement/audit purpose	LOCAL BUSINESS / Coventry process	Review

Where Coventry City Council is the authoritative record holder, Templars should not retain duplicate eligibility information longer than its own legitimate operational/audit need.

PART H — DISPOSAL AND REVIEW

33. Secure Destruction

At the end of the retention period, records will be:

- **DESTROYED** — securely and irreversibly disposed of;
- **TRANSFERRED** — securely passed to the responsible organisation;
- **REVIEWED** — considered to establish whether further retention is justified; or
- **ARCHIVED** — selected deliberately for permanent historical preservation.

Personal or confidential paper records must not be placed in ordinary waste or recycling.

They should be:

- destroyed through an approved confidential-waste service; or
- cross-cut shredded where appropriate.

Electronic records must be securely deleted.

Simply moving a file to a recycle bin, removing a link or closing a user account is not necessarily secure destruction.

Storage devices must be securely sanitised or destroyed through approved ICT/asset-disposal arrangements.

Where an external provider destroys confidential material, appropriate evidence of secure destruction should be obtained.

34. Destruction Log

The school will maintain a record of significant scheduled destruction.



The log should record:

Date Record Category Relevant Date Range / Quantity Method Authorised By Destroyed By / Provider

The destruction log must **not recreate or retain the personal data that has been destroyed**.

A senior leader must authorise scheduled destruction in accordance with school arrangements.

35. Historical and Archival Records

Selected records may be retained permanently where they have genuine enduring historical, evidential or archival value.

Examples might include:

- historic school photographs;
- significant school publications;
- Instrument of Government;
- selected governance material;
- key records relating to major school developments; and
- historically significant school plans or reports.

Personal information must not be kept indefinitely merely because it might be interesting in future.

Where personal information is retained for archival purposes, the school will consider data-protection requirements and appropriate safeguards.

36. Annual Retention Review

This schedule will be reviewed **annually**.

The annual review should include:

- checking changes to legislation and statutory guidance;
- checking the latest DfE school retention guidance;
- checking KCSIE;
- checking relevant DBS, Home Office, HSE, HMRC and ICO guidance;
- checking current Coventry DPO/Local Authority guidance where applicable;
- identifying records whose retention period has expired;
- checking electronic archives and former-user accounts;
- checking that routine backups are not being used as permanent archives;

- 
- identifying unnecessary duplicate records;
 - checking that local retention periods remain proportionate;
 - ensuring privacy notices reflect actual retention arrangements where relevant; and
 - recording destruction appropriately.

Where national statutory guidance specifies a different period from this schedule, the **new legal/statutory requirement takes precedence** and this schedule must be updated.

Appendix 1 — Source and Authority Key

The principal sources underpinning this schedule are:

Department for Education

Data Protection in Schools – Record Keeping and Management

Used for prescribed/current school retention periods including:

- primary pupil records;
- safeguarding records;
- staff allegations;
- finance records;
- admission and attendance registers;
- curricular records;
- educational visits;
- governance records;
- health and safety records;
- property records; and
- staff records.

Keeping Children Safe in Education 2026

Used for:

- safeguarding-file transfers;
- records of allegations against staff;
- distinction between substantiated, unfounded, unsubstantiated, false and malicious allegations;
- DBS certificate retention;

- 
- Single Central Record requirements; and
 - low-level concerns.

School Attendance (Pupil Registration) (England) Regulations 2024

Used in relation to admission and attendance-register requirements.

Education (Pupil Information) (England) Regulations 2005

Used in relation to pupil educational records and transfer.

Limitation Act 1980

Relevant to a number of contractual/evidential periods.

Home Office Right to Work Guidance

Used for:

- retaining right-to-work evidence throughout employment and for two years afterwards.

Disclosure and Barring Service Guidance

Used for:

- DBS certificate handling;
- identity-validation record requirements; and
- secure destruction.

Health and Safety Executive / COSHH Requirements

Used for:

- health surveillance;
- hazardous-substance monitoring; and
- relevant health and safety records.

HMRC

Used where relevant for payroll and VAT records.

Information Commissioner's Office

Used for:

- UK GDPR storage limitation;
- retention decisions where no fixed legal period exists;
- secure destruction;
- CCTV;

- 
- data-protection accountability; and
 - preservation of information relevant to information-rights processes.

Coventry City Council

The school will also take account of current:

- Coventry DPO guidance for schools;
- Coventry information-sharing arrangements;
- Coventry financial procedures; and
- any Local Authority instructions applicable to maintained schools.

Where Coventry acts as the authoritative record holder, Templars will avoid retaining unnecessary duplicate records.

Appendix 2 — Summary of Locally Determined Periods

The following periods are **Templars business-retention decisions rather than statutory periods** and must be specifically reviewed with the DPO as part of the annual review:

- routine teacher working assessment data — current year + 1 year;
- minor behaviour records — current year + 1 year;
- SEND intervention working notes — current year + 1 year;
- provision maps — current year + 3 years;
- unsuccessful admissions — current year + 1 year;
- admission appeals — 6 years;
- governor declarations — tenure + 6 years;
- school policies — current + previous 6 years;
- school improvement/SEF documents — current + 6 years;
- unsuccessful recruitment records — normally 6 months;
- grievances — employment + 6 years;
- general risk assessments — life + 6 years;
- routine CCTV — normally 30 days;
- SAR administrative files — 2 years;
- FOI administrative files — 3 years;
- data-breach files — 6 years;

- 
- complaints — 6 years;
 - visitor records — current academic year + 1 year;
 - contractor visitor records — current year + 3 years;
 - family-support working notes — case closure + 3 years; and
 - routine catering registers — current year + 3 years.

These periods should only continue while the school can demonstrate an appropriate business, legal, safeguarding, accountability or evidential justification for them.