Data Retention and Secure Disposal Policy

Including the Data Retention Schedule

Policy owner	Rosie Aylward, Founder and Data Protection Lead
Approved by	Proprietor, Compass Learning
Version	1.0
Approval date	14 July 2026
Review date	July 2027, or earlier following a material change
Applies to	All staff, contractors, volunteers, systems and records used by Compass Learning

Policy status: approved pre-opening policy. The schedule will be updated when systems, commissioners or awarding arrangements are confirmed.

Contents

1. Purpose

Compass Learning is committed to keeping records only for as long as they are required for a clear educational, safeguarding, contractual, legal or operational purpose. This policy explains how retention periods are selected, how records are reviewed, transferred, archived, anonymised or destroyed, and how Compass Learning demonstrates compliance with the storage limitation and accountability principles of the UK GDPR.

The schedule in Appendix 1 is the organisation's default position. A record must not be destroyed merely because its normal retention period has expired where a safeguarding need, complaint, investigation, audit, insurance matter, legal claim, statutory inquiry or preservation notice requires it to be retained.

2. Scope

This policy applies to records in any format, including:

- learner, parent/carer, SEND, health, attendance, behaviour, safeguarding and qualification records;
- staff, applicant, contractor, volunteer, payroll and safer-recruitment records;
- emails, contact-form submissions, Microsoft Outlook caches, Webador mailbox content and downloaded attachments;
- paper documents, notebooks, photographs, video, audio, visitor logs and printed registers;
- cloud systems, shared drives, local devices, mobile phones, backups, removable media and supplier-held information;
- contracts, finance, insurance, complaints, information-rights, data-breach and governance records.

It applies to the proprietor, employees, temporary staff, contractors, volunteers and any person given access to Compass Learning information.

3. Legal and regulatory framework

This policy is informed by:

- the UK General Data Protection Regulation, particularly the storage limitation, integrity and confidentiality, and accountability principles;
- the Data Protection Act 2018;
- Department for Education guidance on data protection in schools, record keeping and management, updated 9 July 2026;

- Keeping Children Safe in Education and current safeguarding information-transfer requirements;
- the Education (Pupil Information) (England) Regulations 2005 and School Attendance (Pupil Registration) (England) Regulations 2024, where applicable;
- the Limitation Act 1980, Companies Act 2006, tax, payroll, pensions, employment, health and safety and right-to-work requirements;
- awarding-organisation and examination-centre requirements that apply to qualifications delivered by Compass Learning.

Data protection legislation does not prescribe one universal retention period. Compass Learning must be able to justify each period by reference to the purpose of the record, legal requirements, risk, the rights of individuals and whether another organisation is the appropriate long-term record holder.

4. Definitions

Record: Information created, received or held as evidence of an activity, decision, transaction, placement or legal obligation.

Retention period: The period for which a record is kept before review, transfer, anonymisation or secure destruction.

Trigger: The event from which the retention period is calculated, such as the end of a placement, date of an incident or end of a financial year.

Controller: The organisation that decides the purposes and means of processing personal data.

Processor: An organisation processing personal data on the documented instructions of a controller.

Legal hold: A temporary suspension of routine deletion because records may be required for a complaint, claim, investigation, inquiry, audit or safeguarding purpose.

Secure disposal: Deletion or destruction that makes information unreadable and not reasonably capable of reconstruction.

5. Policy principles

1. Records will be retained for a defined purpose and for no longer than is reasonably necessary.
2. Retention periods will be applied consistently across paper, email, cloud storage, local devices and supplier systems.
3. Duplicate and convenience copies will normally be destroyed before the authoritative record.
4. Where Compass acts as a processor, the commissioning controller’s written instructions and contract will take priority, provided they are lawful.
5. Where Compass has independent safeguarding, employment, legal or regulatory responsibilities, it may retain an appropriate record in its own right.
6. Records due for deletion will first be checked for safeguarding relevance, complaints, claims, audits and legal holds.
7. Where long-term analysis is useful, information should be anonymised or aggregated rather than retained in identifiable form.
8. All disposal and significant transfers will be authorised and logged.

6. Responsibilities

The proprietor and Data Protection Lead will:

- maintain this policy, the information asset register and processor/controller records;
- approve changes to retention periods and authorise bulk destruction;
- ensure supplier deletion, export and backup arrangements are understood;
- place and release legal holds;
- coordinate annual reviews and retain a destruction log.

The Designated Safeguarding Lead will:

- approve the transfer, archiving and destruction of child-protection records;

- ensure safeguarding files are transferred separately and securely, with receipt confirmed;
- ensure no safeguarding record is destroyed while it remains relevant to the protection of a child or adult.

All staff and contractors must:

- save substantive records in the approved system rather than relying on an email inbox or personal device;
- delete duplicates, downloads and temporary files when they are no longer needed;
- not destroy records outside the approved process;
- report records that may be subject to a complaint, safeguarding concern, investigation or legal claim;
- follow secure disposal and confidentiality requirements.

7. Controller and processor arrangements

Compass Learning may act as an independent controller for its own business, safeguarding, employment, health and safety and legal records. It may act as a processor where a school, academy trust or local authority commissions a placement and instructs Compass how learner information is to be handled.

Before live learner data is accepted, the relevant agreement must state:

- which organisation is the controller for each category of information;
- the retention period or return/deletion instruction at the end of the placement;
- whether Compass may retain a minimal record for legal, safeguarding, insurance or audit purposes;
- how safeguarding, SEND, attendance and progress information will be transferred;
- how deletion from active systems, Outlook caches, downloads and backups will be handled.

Where the commissioner requires a shorter retention period, Compass will comply unless an independent legal or safeguarding duty requires continued retention. Where a commissioner asks Compass to keep information for longer than the schedule, the request and justification must be documented.

8. Retention, review and legal holds

The retention period starts from the trigger stated in Appendix 1. “Review” does not mean automatic destruction; it means that the record owner must determine whether the record should be destroyed, anonymised, transferred or retained under a documented exception.

A legal hold must be applied where records may be relevant to:

- a safeguarding investigation or statutory inquiry;
- a complaint, subject access request, ICO matter or other information-rights dispute;
- an employment, contractual, personal-injury, negligence or discrimination claim;
- a police, local-authority, awarding-body, insurer, HMRC, Ofsted or regulatory investigation;
- anticipated litigation or a solicitor’s preservation request.

The hold will identify the records and systems affected, the person responsible and the date of review. Routine deletion will resume only when the Data Protection Lead confirms that the hold has ended.

9. Email, cloud systems and backups

The business mailbox info@compass-learning.co.uk is hosted by Webador and accessed through Microsoft Outlook. The mailbox is not the permanent record store. Substantive placement, safeguarding, contract, finance or staff records must be filed into the relevant approved folder or system.

- Routine and transitory emails should be deleted when the task is complete and normally within six months.
- Substantive emails inherit the retention period of the record to which they relate.
- Deleted Items and Junk folders must be cleared regularly.
- Downloaded attachments and Outlook offline caches on authorised devices must be included in deletion and device-leaver procedures.
- Automatic forwarding to personal email accounts is prohibited.
- Highly sensitive learner, EHCP, medical or safeguarding files should be transferred through an approved secure method wherever available.

- Backups are for resilience, not indefinite archiving. Deleted data may remain in protected backups until overwritten through the normal backup cycle, normally no longer than 90 days, unless a legal hold applies.

10. Transfer of learner and safeguarding records

At the end of a placement, Compass will agree with the commissioning school or local authority which learner records must be transferred, returned or retained. The transfer will used the approved secure channel of CPOMS and will keep a record of what was transferred, when, by whom and to whom must be kept.

Child-protection records must:

- be kept separately from the ordinary learner file;
- be transferred securely and separately to the appropriate new school, college or controller;
- be transferred as soon as possible and in accordance with current KCSIE timescales;
- have confirmation of receipt obtained and logged;
- not be sent through ordinary unprotected email where a safer method is available.

Where Compass is not the long-term record holder, working copies will be deleted after transfer is confirmed and the contractual close-down period has expired. Compass may retain a minimal transfer log and any record it needs for its independent safeguarding or legal responsibilities.

11. Secure disposal

Records must not be placed in ordinary waste, recycling bins or an unsecured skip.

Paper records will be:

- destroyed using a cross-cut shredder or an approved confidential-waste contractor;
- kept securely while awaiting destruction;
- covered by a certificate of destruction where an external contractor is used.

Electronic records will be:

- deleted from the active system, mailbox, local device, downloads folder, recycle bin and shared storage;
- removed from synchronised Outlook devices and unauthorised local archives such as PST files;
- securely erased or physically destroyed when equipment or storage media is disposed of;
- allowed to expire from protected backups through the documented backup cycle.

A destruction log will record the record category, date range, volume or file count, retention rule, method, date, authorising person and person or supplier completing the destruction. The log must not reproduce the sensitive content that has been destroyed.

12. Compliance, training and review

- The retention schedule will be reviewed at least annually.
- An earlier review will take place when legislation, DfE or ICO guidance, services, systems, premises, commissioners or awarding arrangements change.
- Staff will receive information-governance training before accessing live personal data and refresher training thereafter.
- Compliance checks will include mailbox housekeeping, downloads, local devices, shared folders, safeguarding records, supplier systems and deletion logs.
- Repeated or deliberate failure to follow this policy may be managed under disciplinary or contractual procedures.

Appendix 1: Data Retention Schedule

Important: Where Compass acts solely as a processor, the commissioning controller's lawful written instructions take priority. The periods below apply to Compass-owned records and provide the default where the contract is silent. A legal hold or safeguarding need overrides routine destruction.

Ref	Record category	Retention period / trigger	Action at end	Reason / operational notes
A1	General website or telephone enquiry not converted to a referral	12 months after final meaningful contact	Destroy securely	Long enough to respond, follow up and evidence the enquiry; do not retain detailed learner information in the general enquiry system.
A2	Webador contact-form submission	12 months after final response, or move to the referral record	Delete from Webador, email and downloads	Contact forms must not be used to collect full EHCP, medical or safeguarding records.
A3	Website analytics, server and cookie information	Provider setting, normally no more than 14 months unless justified	Delete or aggregate	Review Webador and embedded analytics settings annually.
A4	Published photographs, video, testimonials and permission records	Review annually; retain media only while valid and required. Retain evidence of permission for 3 years after last use or withdrawal	Remove from active channels and delete source copies where feasible	Safeguarding restrictions override consent. Public copies may remain in third-party caches beyond Compass control.
A5	Unsuccessful or withdrawn learner referral	12 months after decision or withdrawal	Destroy or anonymise	Retain longer only for a safeguarding concern, complaint, repeated referral pattern or legal hold.
A6	Accepted referral, admission and placement administration	If Compass is record holder: until learner's 25th birthday. If processor: transfer/return at placement end and delete working copies within 3 months of confirmed transfer	Transfer, review and securely destroy	The commissioning agreement must identify the authoritative record holder.
A7	Core learner education record, including Compass-created progress reports and final placement report	If Compass is record holder for a secondary/post-16 learner: until 25th birthday. If processor: return/transfer under contract and delete copies within 3 months	Transfer or secure destruction	A minimal placement index or transfer log may be retained for 6 years to evidence contractual delivery.
A8	Attendance register and attendance entries	6 years from date of entry	Destroy securely	Aligned with DfE school retention guidance. Significant welfare actions also belong in safeguarding or learner records.
A9	Curriculum plans and non-identifiable schemes of work	Current version plus 6 years; permanent retention may be considered for significant organisational records	Review, archive or destroy	Remove learner names and personal information.
A10	Individual learner work samples not required for qualifications	At least 1 year after placement ends; up to 6 years where needed to evidence progress, complaint handling or contractual outcomes	Return to learner, anonymise or destroy	Keep representative samples rather than every piece of work.
A11	Baseline assessments, individual support plans, intervention records and reintegration plans	Follow the core learner record: until 25th birthday if Compass is record holder; otherwise transfer and delete within 3 months	Transfer or destroy	Retain only the versions needed to evidence decisions and progress.

Ref	Record category	Retention period / trigger	Action at end	Reason / operational notes
A12	Copies of EHCPs, SEN support plans and third-party professional reports	Active placement plus up to 3 months after confirmed transfer/return, unless incorporated into a Compass-held core record or subject to legal hold	Return/transfer then destroy working copies	The local authority, school or parent is normally the appropriate long-term holder of the original.
A13	Compass-created SEND assessments and reports	Follow core learner record, normally until 25th birthday if Compass is the record holder	Transfer or destroy	A copy may be provided to the commissioner, parent/carer and learner as appropriate.
A14	Child-protection and safeguarding file	Until child's 25th birthday; where related to child sexual abuse, until 75th birthday	Transfer securely where required; then review and destroy securely	Keep separately from the main learner file. Obtain confirmation of receipt when transferred.
A15	Safeguarding transfer log and receipt confirmation	6 years after placement ends or longer while the related safeguarding file is retained	Destroy securely	The log should identify the file and recipient without repeating sensitive details.
A16	Behaviour incidents, exclusions, serious welfare concerns and risk assessments	6 years after incident or placement end; retain within safeguarding/core learner record until 25 where relevant	Review, transfer or destroy	Safeguarding, injury or police-related records may require longer retention.
A17	Restrictive intervention, restraint or seclusion record in the learner file	Treat as part of the learner or safeguarding file; normally until 25th birthday	Transfer or destroy securely	Maintain the required institutional incident log separately.
A18	Institutional restrictive-intervention incident log	6 years after the incident, with annual review; retain linked child record until 25 where relevant	Archive, anonymise or destroy	Risk-led period reflecting oversight, inspection and potential injury claims.
A19	Learner medical, allergy, medication and care-plan information	Active placement plus 3 months after confirmed transfer/return; incident-related records follow the accident or learner-file period	Transfer and destroy working copies	Keep current information accessible to relevant staff during placement.
A20	Medication administration records	6 years after the last entry; longer if linked to a safeguarding or injury matter	Destroy securely	Retain with incident records where an error or adverse event occurred.
A21	Accident book or RIDDOR record	At least 3 years from date of record	Destroy securely	Accidents involving learners must also be recorded in the pupil/learner record and retained under that record's period.
A22	Educational visit planning, consent and risk-assessment records	10 years from date of visit	Destroy securely	If an incident occurred, retain relevant permissions and reports with the learner/incident record.
A23	Routine transport lists and collection instructions	End of term plus 3 months	Destroy securely	Incident, safeguarding or complaint records are retained under the relevant longer category.
A24	Qualification candidate registration, assessment evidence, internal quality assurance and access-arrangement records	Period required by the awarding organisation or examination centre; default 3 years after certification or last activity if no longer period is specified	Return, archive or destroy securely	Record the exact NOCN, NCFE or centre requirement when approval is obtained.
A25	Certificates and achievement records held by Compass	6 years after certification, or awarding-body requirement	Return to learner where appropriate, then destroy unnecessary copies	Achievement summaries may be part of the core learner record.

Ref	Record category	Retention period / trigger	Action at end	Reason / operational notes
B1	Routine or transitory business email	Delete when task is complete; normally within 6 months	Delete from mailbox, Deleted Items and local downloads	The mailbox is not the permanent filing system.
B2	Substantive learner, safeguarding, contract, HR or finance email	File into the relevant authoritative record and apply that record's retention period	Delete duplicate mailbox copies when no longer required	Avoid sensitive data in subject lines and use secure transfer methods.
B3	Microsoft Outlook local cache, downloaded attachments and PST archives	No longer than the source record; remove immediately from lost, replaced or unauthorised devices	Secure deletion or device wipe	Personal devices and unapproved archives must not be used.
B4	System backups	Normal backup rotation, normally no more than 90 days after source deletion	Automatic overwrite or secure destruction	Backups are not an archive. Restoration procedures must prevent permanently deleted records being silently reintroduced.
B5	Visitor sign-in records	12 months after visit	Destroy securely	Retain longer only if linked to an incident, safeguarding concern or investigation.
B6	CCTV footage, if introduced	Normally 30 days	Automatic overwrite; preserve relevant clips under legal hold	A separate CCTV assessment and privacy notice are required before use.
C1	Complaints and responses	6 years after closure	Destroy securely	Safeguarding, employment or legal-claim material follows the relevant longer period.
C2	Subject access and other information-rights request file	3 years after closure	Destroy securely	Keep identity evidence only as long as needed; retain response and decision trail.
C3	Personal-data breach and security-incident file	6 years after closure	Destroy securely	Allows evidence of accountability, risk assessment, notification and remedial action.
C4	Information audit, asset register, ROPA, DPIA and transfer-risk assessments	Current version plus 6 years after superseded or processing ends	Destroy securely or retain anonymised historical record	Retain versions needed to demonstrate decisions and compliance.
C5	Data-processing agreements, data-sharing agreements and supplier due diligence	6 years after agreement or processing relationship ends	Destroy securely	Longer where a live claim, audit or statutory requirement applies.
C6	Superseded data-protection, safeguarding and operational policies	6 years after superseded	Destroy securely; retain selected historic copies if justified	Current signed policy must remain readily available.
C7	Destruction and transfer logs	6 years after the logged action	Destroy securely	Do not reproduce the sensitive content destroyed or transferred.
D1	Unsuccessful job applications, interview notes and selection records	6 months after recruitment decision	Destroy securely	Extend only where a complaint, dispute or legal hold exists.
D2	Successful application, references, qualifications and recruitment decision record	Transfer to personnel file; retain 6 years after employment ends	Destroy securely	Keep only evidence relevant to the role.
D3	Personnel file, contract, performance, training, grievance and disciplinary records	6 years after employment ends	Destroy securely	Safeguarding allegations and pension records may require longer.
D4	DBS certificate copy or full disclosure information	Normally no more than 6 months after recruitment decision	Destroy immediately by secure means	Retain only permitted check metadata, decision and risk assessment where required.

Ref	Record category	Retention period / trigger	Action at end	Reason / operational notes
D5	DBS check metadata / single central record entry	Duration of employment plus 6 years	Destroy securely	May include check type, date, certificate number, barred-list status and decision, not a copied certificate.
D6	Safeguarding allegations against staff, contractors or volunteers, except malicious/false records removed in accordance with KCSIE	Until normal pension age or 10 years from allegation, whichever is longer	Destroy securely following review	Maintain the clear summary, outcome and reference decision required by current KCSIE.
D7	Low-level concerns about staff	At least until the individual leaves; then review. Retain up to 6 years after employment ends where needed for patterns, misconduct, reference or legal purposes	Destroy securely following documented review	Keep confidentially and separately or within an appropriately restricted staff safeguarding record.
D8	Right-to-work check copies	Duration of employment plus 2 years	Destroy securely	Retain the date the check was completed.
D9	Payroll and PAYE records	3 years from end of tax year	Destroy securely	Minimum-wage evidence is retained for 6 years.
D10	National Minimum Wage records	6 years from the relevant pay-reference period	Destroy securely	Keep sufficient evidence of hours and pay.
D11	Maternity, paternity, adoption and statutory pay records	3 years after end of the tax year to which they relate	Destroy securely	Personnel correspondence may remain in the personnel file where relevant.
D12	Automatic-enrolment pension records	6 years; opt-out records 4 years	Destroy securely	Apply provider and statutory requirements.
D13	Occupational health, sickness and reasonable-adjustment records	6 years after employment ends, unless a longer health-surveillance period applies	Destroy securely	Restrict access and separate detailed medical reports from general personnel records.
D14	Health-surveillance records for hazardous exposure	40 years where applicable	Destroy securely	Only applies if the relevant hazardous-exposure regime arises.
E1	Company accounting records, invoices, receipts, bank statements, annual accounts and company tax records	6 years from end of the relevant company financial year	Destroy securely	Retain longer where HMRC requires it or a transaction spans longer periods.
E2	Contracts with commissioners, suppliers and service providers	6 years from last payment or termination, whichever is later	Destroy securely	Deeds may require 12 years.
E3	Insurance policies, claims and correspondence	6 years after expiry or claim closure; longer where insurer requires or a child/personal-injury matter remains possible	Destroy securely	Employers' liability and safeguarding-related records may justify longer retention.
E4	Proprietor decisions, key governance minutes and annual compliance reviews	10 years	Destroy securely or select for permanent organisational archive	Remove unnecessary personal data from permanent historical records.
E5	Company statutory registers and constitutional records	Life of the company, and as required after dissolution	Transfer to successor, archive or dispose in accordance with company law	Keep authoritative copies secure and current.
E6	Fire risk assessments and accessibility plans	Life of record/plan plus 6 years	Destroy securely	Retain superseded versions where needed to evidence compliance.
E7	Building maintenance, contractor checks and site-compliance records	6 years after superseded, completion or financial year end, depending on record	Destroy securely	Longer statutory periods may apply to specialist exposure or property records.

Appendix 2: Destruction and Transfer Log Requirements

The following fields must be recorded for significant destruction or transfer activity:

- unique log reference;
- date of destruction or transfer;
- record category and date range;
- approximate number of files, boxes or electronic records;
- retention rule and trigger;
- confirmation that legal-hold and safeguarding checks were completed;
- method of destruction or secure-transfer channel;
- name and role of person authorising the action;
- name of person or supplier completing it;
- recipient and receipt-confirmation date for transfers;
- certificate-of-destruction reference where applicable;
- exceptions, errors or follow-up actions.

Minimum transfer evidence: what was sent, the authorised recipient, date and method, sender, and confirmation of receipt. The log must not contain a duplicate narrative of the safeguarding or medical content transferred.

Appendix 3: Reference Sources

- Department for Education, Data protection in schools: Record keeping and management (updated 9 July 2026).
- Information Commissioner's Office, Data storage advice and UK GDPR storage limitation guidance.
- Department for Education, Keeping Children Safe in Education, current statutory guidance.
- Department for Education, Record keeping and retention information for academies and academy trusts.
- Disclosure and Barring Service, Handling of DBS certificate information.
- HM Revenue & Customs, PAYE and payroll for employers: Keeping records; company and accounting records.
- Home Office, Employer's guide to right-to-work checks.
- The Pensions Regulator, records that must be kept under automatic-enrolment duties.
- Information and Records Management Society, Schools Toolkit guidance, including restrictive-intervention records.

Policy review note: This schedule will be checked against each commissioning contract, awarding-body agreement and the systems actually selected before live learner data is processed.