Document Name	Records management, retention, secure storage and disposal			
Document Number				
Issue Date	Revision	Review Date	Policy Owner	Signature
01/01/2026	01	01/01/2029	Emily Boyd on behalf of Silvergrove Home Care	

1. Purpose

The purpose of this policy is to ensure that Silvergrove Home Care creates, keeps, stores, retrieves, shares, archives and disposes of records in a lawful, secure and consistent way. The policy supports continuity of care, regulatory compliance, good governance, data protection, safeguarding and defensible decision-making. This policy is available to Service Users and / or their representatives.

2. Scope

This policy applies to all records created, received or maintained by Silvergrove Home Care in the course of delivering domiciliary care and running the business, regardless of format. It covers paper records, electronic files, emails, scanned copies, photographs, text-based care systems, cloud folders and any other medium used to record business or care information.

- Service user records including assessments, care plans, risk assessments, visit notes, medication support records, safeguarding records and communications about care.
- Operational and business records including rosters, invoices, contracts, complaints, incidents, audits, policies, training records and financial records.
- Records handled by employees, contractors, managers and third-party processors acting on behalf of Silvergrove Home Care.

3. Principles

- Records must be accurate, complete, timely, legible and attributable to the person creating or updating them.
- Records containing personal or special category data must be protected against unauthorised access, loss, alteration, disclosure or destruction.
- Personal data must not be retained for longer than necessary and retention decisions must be justifiable by operational, regulatory, contractual or legal need.
- Where records are not covered by the schedule in this policy, managers must document the retention decision, rationale and approval.

- Where litigation, a complaint, safeguarding enquiry, regulatory inspection, insurance issue or data access issue is ongoing or anticipated, relevant records must be preserved until the matter is fully concluded.

4. Roles and responsibilities

Role	Key responsibilities
Directors / Service Provider /Home Care Manager	Approve this policy, allocate resources, oversee compliance and ensure a clear governance route for exceptions, legal holds and destruction decisions.
Home Care Manager	Ensure staff follow local procedures, maintain secure storage arrangements, monitor retention, authorise disposal and keep evidence of training, audits and destruction activity.
All staff and contractors	Create accurate records, use approved systems only, keep information confidential, report incidents promptly and never destroy or remove records without authorisation.
Data protection lead / nominated manager	Provide advice on GDPR, data subject rights, breaches, data sharing and retention questions, and support review of high-risk or exceptional cases.

5. Record creation, storage and access

- Records must be created as close as possible to the event, visit, contact or decision they describe.
- Paper files must be stored in locked cabinets or rooms with controlled access. Files must not be left in unattended vehicles or open areas.
- Electronic records must be stored on approved systems with password protection, role-based access, encryption where available and appropriate backup arrangements.
- Use of personal devices, personal email accounts or unapproved consumer apps for storing service user information is prohibited unless expressly authorised under a secure company process.
- Access to records must be limited to those with a legitimate work need. Access should be traceable where systems allow.

6. Retention and disposal rules

The schedule below sets minimum retention periods for core Silvergrove Home Care records. Where another law, insurer, regulator, contract or active case requires longer retention, the longer period applies. Destruction must be confidential, authorised and logged.

Record category	Examples	Why kept	Minimum retention	Final action
Service user care record	Assessment, care plan, reviews, contact notes, body maps, consent forms, key correspondence	Adult service user	8 years after last contact or end of service	Secure destruction unless legal or safeguarding hold applies
Medication support record	MAR sheets, medication	Care delivery / safety	8 years after last entry	Secure destruction

	assistance/refusal records, incident follow-up			
Clinical / service risk assessment	Falls, moving and handling, skin integrity, nutrition, lone worker and environmental risk records	Care and safety	8 years after last entry	Secure destruction
Safeguarding record	Concerns, referrals, investigation material, protection planning and outcomes	Highly sensitive	Retain for at least 10 years after case closure; longer where required by regulator or legal advice	Archive or destroy under formal authorisation
Incident / accident record	Service user, staff or visitor incident reports, witness accounts, investigation findings	Operational / legal	10 years from closure; exposure-related incidents may require longer	Secure destruction
Complaint record	Complaint correspondence, investigation notes, response letters and learning actions	Operational / legal	7 years after closure	Secure destruction
Staff personnel file	Employment contract, vetting, references, performance and core employment records	HR / confidential	Employment duration plus 7 years	Secure destruction unless pension/archive need applies
Recruitment file - unsuccessful candidate	Application, interview notes, checks and selection records	HR / confidential	1 year after recruitment campaign closes	Secure destruction
Training and competency record	Induction, mandatory training, supervision and competency sign-off	HR / compliance	Employment duration plus 7 years	Secure destruction
Rota, timesheet and visit verification	Staff rosters, worked hours, call monitoring and visit confirmation	Operational / payroll	Current year plus 6 years	Secure destruction
Payroll, tax and finance records	Payroll data, invoices, receipts, bank support, tax and accounting records	Financial / confidential	Current year plus 6 years	Secure destruction
Insurance and claims file	Public liability, employer liability, motor, incident claim	Legal / insurance	Claim closure plus 6 years; policy documents may be kept longer	Archive or secure destruction

	correspondence and settlement records			
Contracts and supplier files	Service agreements, processor contracts, supplier due diligence and procurement records	Commercial / governance	Contract term plus 6 years	Secure destruction
Data protection request / breach record	SARs, rectification/erasure requests, breach logs and DPC correspondence	Compliance / confidential	6 years after closure, except routine requests that may be retained for 1 year where risk is low	Secure destruction
Governance records	Board minutes, major policy approvals, annual quality reports and key audit reports	Corporate / governance	Permanent or long-term archive as decided by management	Archive
CCTV record (if used)	Routine security footage not linked to an incident	Security	30 to 90 days unless required for investigation	Automatic overwrite or secure deletion
Destruction log	Register of records disposed of, authorisation and method	Compliance evidence	Permanent	Retain securely

7. Destruction and destruction log

- Paper records must be shredded or destroyed through a confidential waste provider. Electronic records must be securely deleted from live systems, shared drives and portable media, subject to backup and system controls.
- A destruction log must record the record category, date range, retention rule, disposal date, disposal method, approver and person supervising disposal.
- No record may be destroyed where there is an active complaint, safeguarding issue, coronial matter, insurance claim, regulatory inspection, legal action or formal request for access.

8. Digitisation and duplicate records

Where paper records are scanned into an approved electronic system, Silvergrove must ensure the digital copy is complete, legible, secure and retrievable. Original paper records should not be destroyed until quality checks are complete and the organisation is satisfied that the scanned version is the reliable record. Duplicate copies should not be retained longer than necessary.

9. Data subject rights, confidentiality and information sharing

- Requests for access, correction, restriction or other data rights must be handled under Silvergrove Home Care data protection procedures.
- Information sharing with GPs, hospitals, family members, commissioners, regulators or external professionals must be lawful, necessary, proportionate and appropriately documented.

- Special category data must be shared only where there is a clear lawful basis and an operational need or safeguarding duty.

10. Monitoring, training and review

- Managers should review retention and storage practices at least annually and after any serious incident, audit finding or regulatory recommendation.
- Relevant staff must receive induction and refresher training on record keeping, confidentiality, retention and secure disposal.
- This policy should be reviewed every three years, or earlier where legislation, guidance, technology or service arrangements change.

Appendix A - Good practice checklist

- Write records promptly and objectively.
- Date, time and sign or authenticate entries.
- Do not overwrite or obscure original entries; correct errors transparently.
- Store paper and electronic files only in approved locations.
- Report lost, misdirected or unauthorised disclosures immediately.
- Check the retention schedule before disposing of any record.