RECORDS MANAGEMENT AND RECORD KEEPING POLICY

PRN-109: Records Management and Record Keeping Policy
Company Name: AI Auto-Tech Ltd
Trading/Business Name: CAREHOPES
Company Registration Number: 15556946
SIC Code: 88100 – Social Work Activities Without Accommodation for the Elderly and Disabled
Email: admin@carehopes.com
Version Number: V01 20260815
Date of Review: (August 2026)

---

1. Purpose

The purpose of this policy is to ensure that the organisation creates, maintains, stores, accesses, retains, and disposes of records in a consistent, secure, accurate, and lawful manner.

The organisation recognises that effective record keeping is essential for:

- Safe and effective service delivery
- Safeguarding adults
- Accountability and transparency
- Regulatory compliance
- Risk management
- Business continuity
- Organisational learning
- Protection of service users, employees, and volunteers

Accurate records contribute to person-centred support and demonstrate the quality and integrity of services provided.

---

2. Scope

This policy applies to:

- Employees

- Volunteers
- Directors
- Trustees
- Managers
- Contractors where applicable

The policy applies to all records held by the organisation, including:

- Service user records
- Volunteer records
- Employee records
- Safeguarding records
- Incident reports
- Financial records
- Training records
- Policies and procedures
- Governance records
- Electronic and paper-based records

---

3. Policy Statement

The organisation is committed to ensuring that records are:

- Accurate
- Complete
- Clear
- Secure
- Accessible to authorised persons
- Kept up to date
- Retained appropriately
- Disposed of securely

Records must support effective decision-making, accountability, and service quality.

---

4. Legal Framework

This policy is guided by:

- Data Protection Act 2018
- UK GDPR
- Care Act 2014
- Health and Safety at Work etc. Act 1974
- Human Rights Act 1998
- Equality Act 2010
- Common Law Duty of Confidentiality

---

5. Objectives

The objectives of this policy are to:

- Promote good record keeping practices.
- Ensure information is reliable and accessible.
- Protect confidential information.
- Meet legal and regulatory requirements.
- Support safeguarding responsibilities.
- Enable effective service delivery.
- Support business continuity arrangements.

---

6. Definition of a Record

A record is any information created, received, held, or maintained by the organisation as evidence of its activities.

Records may include:

- Written documentation
- Electronic files
- Emails

- Text messages
- Reports
- Risk assessments
- Safeguarding records
- Meeting minutes
- Photographs
- Financial documents
- Training records

---

7. Principles of Good Record Keeping

All records should be:

Accurate

Information must be factual and correct.

Clear

Records should be understandable and easy to follow.

Timely

Records should be completed as soon as possible after events occur.

Relevant

Only necessary information should be recorded.

Objective

Records should distinguish facts from opinions.

Secure

Information must be protected from unauthorised access.

---

8. Responsibilities

Directors

Responsible for:

- Governance oversight.

- Ensuring compliance with legal requirements.
- Supporting effective record management systems.

Managers

Responsible for:

- Monitoring record keeping standards.
- Ensuring records are maintained appropriately.
- Supporting training and compliance.
- Undertaking audits where required.

Employees and Volunteers

Responsible for:

- Creating accurate records.
- Following organisational procedures.
- Maintaining confidentiality.
- Storing records securely.
- Reporting concerns relating to records.

---

9. Service User Records

The organisation will maintain records relevant to service delivery.

Records may include:

- Personal details
- Emergency contacts
- Consent records
- Support plans
- Risk assessments
- Safeguarding concerns
- Contact notes

- Significant events

Records should reflect the support provided and any actions taken.

---

10. Recording Standards

Records must:

- Be written clearly.
- Be factual.
- Be professional.
- Be respectful.
- Avoid discriminatory language.
- Be signed or attributable to the person creating the record where appropriate.

Employees and volunteers should avoid:

- Personal opinions
- Speculation
- Assumptions
- Inappropriate comments

---

11. Electronic Records

Electronic records may include:

- Databases
- Digital files
- Emails
- Electronic forms
- Secure cloud-based systems

Electronic records must be:

- Password protected.
- Securely stored.
- Accessible only to authorised individuals.

- Backed up where appropriate.

---

12. Paper Records

Paper records must be:

- Stored securely.
- Protected from damage.
- Protected from unauthorised access.
- Retained in accordance with organisational procedures.

Secure storage arrangements should be used wherever appropriate.

---

13. Confidentiality

Records often contain sensitive and confidential information.

Employees and volunteers must:

- Maintain confidentiality.
- Access information only when authorised.
- Prevent unauthorised disclosure.
- Follow the Confidentiality Policy.

Confidential information must not be discussed or shared inappropriately.

---

14. Data Protection and Security

The organisation will take appropriate measures to protect information from:

- Loss
- Theft
- Damage
- Unauthorised access
- Unauthorised disclosure
- Misuse

Security measures may include:

- Password protection
- Encryption
- Locked storage
- Access controls
- Secure disposal procedures

---

15. Access to Records

Access to records will be restricted to individuals with a legitimate need to know.

Access may be granted to:

- Relevant employees
- Relevant volunteers
- Managers
- Regulatory or legal bodies where required

Unauthorised access is prohibited.

---

16. Record Amendments

Where amendments are required:

- Original information should remain identifiable.
- Changes should be dated.
- Reasons for amendment should be clear.
- Records should not be falsified or altered improperly.

The integrity of records must always be maintained.

---

17. Retention of Records

Records will be retained for appropriate periods based on:

- Legal requirements.
- Organisational needs.
- Safeguarding considerations.

- Regulatory guidance.

A retention schedule will be maintained where appropriate.

Records should not be retained longer than necessary.

---

18. Secure Disposal of Records

When records reach the end of their retention period, they must be disposed of securely.

Examples include:

Paper Records

- Confidential shredding
- Secure destruction

Electronic Records

- Permanent deletion
- Secure destruction of storage devices where appropriate

Disposal must prevent reconstruction or unauthorised access.

---

19. Record Keeping and Safeguarding

Accurate record keeping is essential for safeguarding.

Safeguarding records should:

- Be factual and timely.
- Clearly document concerns.
- Record actions taken.
- Record referrals made.
- Be stored securely.

Poor record keeping can place individuals at risk and impair safeguarding investigations.

---

20. Record Keeping and Incident Reporting

Records relating to incidents should include:

- Date and time
- Individuals involved
- Description of events
- Actions taken
- Follow-up arrangements

Incident records should support investigation, learning, and accountability.

---

21. Auditing and Quality Assurance

The organisation may undertake periodic audits to review:

- Accuracy of records
- Completeness of documentation
- Compliance with policies
- Information security arrangements
- Retention and disposal practices

Audit findings will be used to improve record management practices.

---

22. Training

Employees and volunteers will receive training appropriate to their role regarding:

- Record keeping standards
- Data protection
- Confidentiality
- Information security
- Safeguarding documentation
- Incident recording

Training needs will be reviewed regularly.

---

23. Record Keeping Errors

Where record keeping errors are identified:

- Corrections should be made promptly.
- Risks should be assessed.
- Appropriate management oversight should be provided.
- Learning opportunities should be identified.

Serious concerns may require investigation under relevant organisational procedures.

---

24. Case Study

Scenario: Recording a Safeguarding Concern

A volunteer becomes concerned that a service user may be experiencing financial exploitation.

Action Taken

The volunteer:

- Records the concern immediately.
- Documents observed facts only.
- Avoids assumptions.
- Reports the concern to the Designated Safeguarding Lead.

Outcome

A safeguarding referral is made based upon clear and accurate documentation.

Learning Point

Timely and factual records support effective safeguarding and decision-making.

---

25. Monitoring and Quality Assurance

The organisation will monitor:

- Record keeping standards
- Data breaches
- Safeguarding documentation
- Incident reports
- Audit findings

- Staff training compliance

Monitoring results will be used to improve record management systems and practices.

---

26. Responsibilities Summary

Role	Key Responsibilities
Directors	Governance oversight and compliance
Managers	Monitoring, audits and staff support
Employees	Accurate and timely record keeping
Volunteers	Following record keeping procedures

---

27. Review Arrangements

This policy will be reviewed:

- Annually
- Following significant incidents
- Following data breaches
- Following safeguarding reviews
- Following legislative or regulatory changes

Related Policies

- Data Protection and GDPR Policy
- Confidentiality Policy
- Adult Safeguarding Policy
- Incident Reporting Policy
- Business Continuity and Emergency Planning Policy
- Risk Assessment Policy
- Volunteer Management Policy
- Health and Safety Policy