CONFIDENTIALITY POLICY

PRN-32: Confidentiality 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 all information obtained by the organisation is handled responsibly, lawfully, securely, and confidentially.

As a Non-Accommodation Companionship and Wellbeing Support Service for Older People and Adults with Disabilities, the organisation recognises that service users place significant trust in employees and volunteers. Maintaining confidentiality is essential for protecting privacy, dignity, safeguarding, and maintaining confidence in our service.

This policy establishes standards for:

- Collecting information
- Using information
- Sharing information
- Storing information
- Protecting information
- Disclosing information appropriately

---

2. Scope

This policy applies to:

- Employees
- Volunteers
- Directors
- Trustees
- Contractors
- Agency workers
- Students and placements

This policy applies to all information obtained during:

- Home visits
- Wellbeing visits
- Community support activities
- Telephone support
- Volunteer activities
- Support planning
- Safeguarding investigations
- Employment and volunteer management

---

3. Policy Statement

The organisation is committed to:

- Respecting individuals' rights to privacy.
- Protecting confidential information.
- Sharing information appropriately and lawfully.
- Complying with UK GDPR and Data Protection Act 2018 requirements.
- Promoting trust between service users, staff, volunteers, and the organisation.
- Maintaining high professional and ethical standards.

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

---

4. Guiding Principles

The organisation will operate in accordance with the following principles:

Respect

Individuals have the right to expect that personal information will be treated confidentially.

Need-to-Know

Information will only be shared with individuals who require it for legitimate purposes.

Minimum Necessary Information

Only the information required for a specific purpose will be shared.

Accountability

Everyone is responsible for maintaining confidentiality.

Safeguarding

Confidentiality must never prevent action being taken to protect someone from harm.

---

5. What is Confidential Information?

Confidential information includes any information that is not publicly available and relates to an identifiable individual or organisation.

Examples include:

Service User Information

- Names
- Addresses
- Telephone numbers
- Email addresses
- Health information
- Disability information
- Support plans
- Risk assessments
- Financial circumstances

- Safeguarding concerns

Employee and Volunteer Information

- Personnel records
- Contact details
- Payroll information
- Health records
- Performance information

Organisational Information

- Contracts
- Financial records
- Strategic plans
- Internal correspondence
- Policies under development

---

6. Collecting Information

Information will only be collected where it is:

- Relevant
- Necessary
- Proportionate
- Lawful

Individuals will, wherever possible, be informed:

- Why information is being collected
- How it will be used
- Who it may be shared with
- How it will be stored
- Their rights regarding the information

---

7. Access to Information

Access to confidential information will be restricted to authorised individuals.

Employees and volunteers should only access information:

- Necessary for their role
- Required for service delivery
- Required for safeguarding
- Required by law

Unauthorised access to information may result in disciplinary action.

---

8. Use of Information

Information must only be used for legitimate organisational purposes.

Information must not be:

- Accessed out of curiosity
- Shared inappropriately
- Used for personal gain
- Used to discriminate against individuals

All information should be handled professionally and respectfully.

---

9. Information Sharing

Information should only be shared where:

- Consent has been obtained.
- Sharing is necessary for service delivery.
- There is a safeguarding concern.
- There is a legal obligation to share.
- There is a serious risk to an individual or others.

Whenever information is shared, staff should consider:

- Is sharing necessary?
- Is sharing lawful?
- Is sharing proportionate?

- Has only relevant information been disclosed?

Where possible, information sharing decisions should be recorded.

---

10. Consent

Where consent is required, it should be:

- Freely given
- Informed
- Specific
- Unambiguous

Individuals should understand:

- What information is being shared
- Why it is being shared
- Who it is being shared with

Consent may be withdrawn unless another lawful basis applies.

---

11. Limits of Confidentiality

Confidentiality is not absolute.

Information may need to be shared without consent where:

- Abuse or neglect is suspected.
- A person is at risk of serious harm.
- A crime has been committed.
- Public protection concerns exist.
- Legal obligations require disclosure.
- A court orders disclosure.

Employees and volunteers must never promise absolute secrecy.

Individuals should be informed of the limits of confidentiality whenever possible.

---

12. Safeguarding and Confidentiality

Protecting individuals from harm takes priority over confidentiality.

Information must be shared with appropriate persons where there are concerns regarding:

- Physical abuse
- Emotional abuse
- Sexual abuse
- Financial abuse
- Neglect
- Self-neglect
- Domestic abuse
- Modern slavery
- Exploitation

Employees and volunteers must report safeguarding concerns immediately in accordance with the Adult Safeguarding Policy.

---

13. Mental Capacity and Confidentiality

Where an individual lacks capacity to make decisions about information sharing, decisions should be made in accordance with:

- The Mental Capacity Act 2005
- Best-interest principles
- Relevant legal guidance

Where appropriate, information may be shared with:

- Attorneys
- Deputies
- Advocates
- Relevant professionals

Any sharing should be necessary, proportionate, and in the individual's best interests.

---

14. Confidential Discussions

Employees and volunteers must take care when discussing confidential information.

Confidential matters should not be discussed:

- In public places
- On public transport
- In cafes or restaurants
- In lifts or communal areas
- With friends or family members
- With individuals who do not need to know

Private conversations should take place where confidentiality can be maintained.

---

15. Record Keeping

All records must be:

- Accurate
- Factual
- Legible
- Timely
- Relevant
- Secure

Records should contain information necessary for service delivery and organisational purposes.

Employees and volunteers must not alter, remove, destroy, or falsify records.

---

16. Storage and Security of Information

Confidential information must be protected from:

- Loss
- Damage
- Theft
- Unauthorised access

- Unauthorised disclosure

Paper Records

Paper records should:

- Be stored securely.
- Be kept in locked cabinets where appropriate.
- Not be left unattended.

Electronic Records

Electronic records should:

- Be password protected.
- Use secure systems.
- Be accessible only to authorised users.
- Be backed up appropriately.

---

17. Email, Telephone and Electronic Communications

Employees and volunteers must take particular care when communicating electronically.

They must:

- Verify email recipients before sending information.
- Use approved communication systems.
- Protect passwords and login details.
- Avoid sending excessive personal information.
- Report mistakes immediately.

Telephone conversations involving confidential information should be conducted in private wherever possible.

---

18. Social Media and Confidentiality

Employees and volunteers must not:

- Share information about service users online.
- Post photographs of service users without authorised consent.

- Discuss confidential organisational matters.
- Identify service users directly or indirectly.
- Share information that could compromise privacy or dignity.

These requirements apply during and outside working hours.

Professional boundaries must be maintained at all times.

---

19. Family Members, Carers and Representatives

Family members and carers may request information regarding a service user.

Information should only be shared where:

- The service user has given consent.
- There is lawful authority to share.
- The individual lacks capacity and sharing is in their best interests.
- Safeguarding or legal requirements apply.

Family members do not automatically have access to confidential information.

The wishes of the service user should remain central wherever possible.

---

20. Confidentiality Agreements

All employees and volunteers may be required to sign a confidentiality agreement as part of their induction process.

The agreement confirms their responsibility to:

- Protect confidential information.
- Follow organisational policies.
- Maintain confidentiality after leaving the organisation.

Confidentiality obligations continue after employment or volunteering ends.

---

21. Confidentiality Breaches

Examples of confidentiality breaches include:

- Discussing service users in public.

- Sharing information with unauthorised persons.
- Sending information to incorrect recipients.
- Losing records.
- Leaving records unattended.
- Accessing information without authority.
- Publishing confidential information online.

Breaches may be investigated under disciplinary procedures.

---

22. Reporting Confidentiality Breaches

Any actual or suspected breach must be reported immediately.

Employees and volunteers should:

Step 1

Take reasonable action to minimise further disclosure.

Step 2

Inform their manager immediately.

Step 3

Complete an Incident Report Form.

Step 4

Co-operate with any investigation.

Prompt reporting helps minimise harm and ensures legal obligations can be met.

---

23. Whistleblowing and Confidentiality

Employees and volunteers are encouraged to report concerns regarding:

- Poor practice
- Unlawful information sharing
- Data breaches
- Misuse of confidential information
- Safeguarding failures

Concerns should be raised in accordance with the Whistleblowing Policy.

Individuals raising genuine concerns in good faith will be protected from victimisation.

---

24. Training

All employees and volunteers will receive training on:

- Confidentiality
- Data protection
- Information sharing
- GDPR awareness
- Record keeping
- Safeguarding responsibilities
- Professional boundaries

Training will be refreshed periodically and monitored through supervision and appraisal.

---

25. Case Study

Scenario: Disclosure of Safeguarding Information

A companionship volunteer learns that a service user is being financially exploited by a relative.

The service user asks the volunteer not to tell anyone.

Appropriate Response

The volunteer explains that they cannot keep information secret where someone may be at risk of harm.

The volunteer:

- Reports the concern immediately.
- Records the disclosure accurately.
- Follows safeguarding procedures.

Learning Point

Confidentiality must never prevent action being taken to safeguard an individual from abuse or exploitation.

---

26. Responsibilities

Directors

Responsible for:

- Governance oversight.
- Ensuring legal compliance.
- Supporting a culture of confidentiality.

Managers

Responsible for:

- Implementing this policy.
- Providing guidance.
- Monitoring compliance.
- Investigating breaches.

Employees and Volunteers

Responsible for:

- Protecting confidential information.
- Following organisational procedures.
- Reporting concerns promptly.
- Attending mandatory training.

---

27. Monitoring and Review

The organisation will monitor:

- Confidentiality breaches
- Data protection incidents
- Complaints relating to confidentiality
- Training compliance
- Record keeping standards
- Information sharing practices

Findings will be used to improve organisational systems and reduce risks.

---

28. Review Arrangements

This policy will be reviewed:

- Annually
- Following significant incidents
- Following legislative changes
- Following audits or investigations
- Following recommendations from safeguarding reviews

Related Policies

- Data Protection and GDPR Policy
- Adult Safeguarding Policy
- Mental Capacity Act Policy
- Incident Reporting Policy
- Whistleblowing Policy
- Dignity and Respect Policy
- Risk Assessment Policy
- Financial Safeguarding Policy