Consent Documentation Policy

PRN-34: Consent Documentation 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. Introduction

Consent is a foundational safeguarding requirement within CAREHOPES (TC). It protects clients, companions, and the organisation by ensuring that all actions involving client property, personal information, digital interactions, or environmental access are authorised, documented, and compliant with UK law.

This policy establishes the standards, procedures, and documentation requirements for obtaining, recording, storing, and managing client consent.

2. Purpose of the Policy

The purpose of this policy is to:

- ensure all consent is properly documented
- protect client autonomy and rights
- prevent unauthorised actions
- ensure GDPR-compliant storage of consent records
- standardise consent procedures across TC
- support safeguarding and legal compliance
- protect companions from allegations or risk

3. Scope

This policy applies to:

- companions
- volunteers
- staff engaged in client-facing duties

- supervisors responsible for reviewing consent documentation

4. Definitions

4.1. Consent

A client's voluntary, informed, and explicit agreement to allow a companion to perform a specific action.

4.2. Written Consent

Consent documented in writing, signed and dated by the client, and logged in TC's system.

4.3. Digital Consent

Consent provided electronically through TC's approved digital forms or platforms.

4.4. Consent Log

A secure record maintained by TC documenting all consent obtained for client-related actions.

4.5. Sensitive Consent

Consent required for actions involving personal data, property access, digital interactions, or safeguarding-related activities.

5. Roles & Responsibilities

5.1. Companion Responsibilities

Companions must:

- obtain consent before performing any action requiring authorisation
- ensure consent is written, signed, dated, and logged
- forward all consent documentation to the Service Manager
- avoid performing any action without proper consent
- escalate concerns about unclear or withdrawn consent
- maintain professional boundaries

5.2. Supervisor Responsibilities

Supervisors must:

- review consent documentation
- ensure proper storage under GDPR

- verify that consent is valid and complete
- respond to concerns or disputes
- ensure companions follow consent procedures

6. Actions Requiring Written Consent

Companions must obtain written consent for:

6.1. Recording

- photos
- videos
- audio recordings
- recording client property or environment

6.2. Digital Assistance

- setting up accounts
- accessing digital platforms
- assisting with online forms
- facilitating video calls

6.3. Property Access

- entering private rooms
- accessing locked areas
- handling client belongings

6.4. Travel Activities

- domestic travel
- international travel
- holiday companionship
- activity participation

6.5. Environmental Documentation

- photographing hazards
- documenting damage
- reporting environmental concerns

6.6. Any Action Involving Personal Data

- sharing information
- storing information
- transmitting information

7. Consent Requirements

All consent must be:

- **written**
- **signed**
- **dated**
- **specific to the action**
- **time-bound**
- **logged in TC's system**
- **forwarded to the Service Manager**
- **stored securely under GDPR**

Verbal consent is **not sufficient** for any action involving risk, privacy, or digital interaction.

8. Validity of Consent

8.1. Informed Consent

Clients must understand:

- what they are consenting to
- why the action is needed
- how the action will be performed
- any risks involved
- their right to refuse

8.2. Voluntary Consent

Consent must be:

- freely given
- without pressure

- without manipulation
- without coercion

8.3. Time-Bound Consent

Consent is valid only for:

- the specific action
- the specific date
- the specific purpose

Consent does **not** carry over to future actions.

9. Withdrawal of Consent

Clients may withdraw consent at any time.

Companions must:

- stop the action immediately
- document the withdrawal
- notify the Service Manager
- ensure no further related actions occur

Failure to respect withdrawn consent is **gross misconduct**.

10. Prohibited Actions Without Consent

Companions must **never**:

- record clients or their property
- enter private rooms
- handle personal belongings
- assist with digital accounts
- perform digital transactions
- share client information
- store client data
- take photos for documentation
- access confidential documents

These actions constitute **gross misconduct**.

11. Documentation Procedures

11.1. Consent Form Completion

Consent forms must include:

- client name
- companion name
- description of the action
- reason for the action
- date and time
- client signature
- companion signature
- supervisor verification (if required)

11.2. Logging Consent

Companions must:

- upload consent to TC's secure system
- label the consent clearly
- ensure accuracy
- avoid storing consent on personal devices

11.3. Forwarding Consent

All consent must be forwarded to:

Service Manager CAREHOPES (TC)

11.4. Secure Storage

Consent must be stored:

- securely
- digitally encrypted
- accessible only to authorised staff
- compliant with GDPR

12. Safeguarding Requirements

Consent is a safeguarding tool.

Companions must:

- ensure clients are not pressured
- report concerns about forced consent
- escalate signs of exploitation
- avoid actions that compromise client autonomy
- ensure vulnerable clients receive additional support

13. Legal & Regulatory Compliance

This policy aligns with:

- UK GDPR
- Data Protection Act 2018
- UK safeguarding legislation
- TC Confidentiality Policy
- TC Digital Security Policy

Companions must comply with all legal and organisational requirements.

14. Disciplinary Consequences

Non-compliance may result in:

- retraining
- formal warnings
- suspension
- removal from client assignments
- termination
- safeguarding escalation
- legal referral

Unauthorised actions involving client data or property are treated as **gross misconduct**.

15. Amendments

TC may update this policy to reflect:

- legal changes

- safeguarding updates
- operational improvements
- governance decisions

Updates will be communicated through official TC channels.