

Use of Phone & Personal Gadget Policy

PRN-143: Use of Phone & Personal Gadget Policy

Company Name: AI Auto-Tech Ltd

Trading/Business Name: Trusted Companionship

Company Registration Number: 15556946

SIC Code: 88100 – Social Work Activities Without Accommodation for the Elderly and Disabled

Email: info@trustedcompanionship.com

Version Number: V01 20260815

Date of Review: (August 2026)

1. Introduction

The use of phones, tablets, and personal gadgets during companionship must be carefully controlled to protect client privacy, uphold safeguarding standards, and maintain professional boundaries. This policy establishes strict rules governing device use, digital interactions, recording permissions, and data protection during companionship sessions.

2. Purpose of the Policy

The purpose of this policy is to:

- protect client privacy and property
- prevent digital exploitation or misuse
- ensure GDPR-compliant handling of digital content
- establish clear boundaries for device use
- prevent financial or digital manipulation
- safeguard companions from allegations or risk
- standardise consent documentation procedures

3. Scope

This policy applies to:

- companions
- volunteers
- staff engaged in client-facing duties
- supervisors overseeing digital conduct

4. Definitions

4.1. Personal Gadget

Any device owned by the companion, including phones, tablets, laptops, smartwatches, or cameras.

4.2. Client Device

Any device owned by the client, including phones, tablets, laptops, televisions, or digital assistants.

4.3. Digital Transaction

Any online purchase, banking activity, money transfer, or financial operation performed using a digital device.

4.4. Recording

Any audio, video, or photographic capture of client property, environment, or person.

5. Roles & Responsibilities

5.1. Companion Responsibilities

Companions must:

- use devices professionally
- protect client privacy
- avoid handling client finances
- document consent properly
- escalate digital safeguarding concerns
- avoid storing client data on personal devices

5.2. Supervisor Responsibilities

Supervisors must:

- review consent documentation
- respond to digital safeguarding concerns
- ensure companions are trained in digital safety
- enforce compliance with this policy

6. Recording Rules

6.1. Prohibition Without Consent

Companions must **never record client property, environment, or person** without:

- written consent
- signed consent

- dated consent
- logged consent
- consent forwarded to the Service Manager

6.2. Acceptable Recording Purposes

Recording may only occur for:

- documentation of damage
- safeguarding evidence
- client-requested digital tasks
- video call setup (if consented)

6.3. Prohibited Recording Purposes

Companions must not record:

- for personal use
- for social media
- for entertainment
- for private storage
- without explicit consent

Unauthorised recording constitutes **gross misconduct**.

7. Use of Client Devices

Companions must **never**:

- use client phones
- use client tablets
- use client laptops
- access client emails
- access client social media
- access client banking apps
- perform digital transactions
- store client passwords
- store client data

These actions create safeguarding and financial risk.

7.1. Permitted Interaction

Companions may:

- guide clients verbally on how to use their devices
- demonstrate steps on their own device (if safe)
- assist clients in navigating apps **without touching the client's device**

8. Digital Transactions

Companions must **never**:

- use client credit or debit cards
- perform online purchases
- transfer money
- pay bills
- access banking apps
- store card details
- enter PINs or passwords
- handle cash for digital purposes

Financial involvement constitutes **gross misconduct** and may lead to legal escalation.

9. Data Protection & GDPR Compliance

9.1. Prohibited Data Storage

Companions must not store:

- client photos
- client videos
- client documents
- client contact details
- client passwords
- client medical information

on any personal device.

9.2. Secure Handling

All digital interactions must comply with:

- UK GDPR

- Data Protection Act 2018
- TC Confidential Information Management Policy
- TC Digital Security Policy

10. Guidance-Only Rule

Companions may:

- verbally guide clients on device use
- assist with digital literacy
- help set up video calls
- help clients navigate apps
- help clients access online services

Companions must **not**:

- operate devices on behalf of clients
- enter personal information
- manage accounts
- create passwords
- store login details

11. Safeguarding Requirements

Companions must:

- report suspicious digital activity
- escalate concerns about financial exploitation
- notify TC if a client is being digitally manipulated
- avoid involvement in client digital disputes
- avoid accessing sensitive digital content

Digital safeguarding concerns must be escalated immediately.

12. Documentation Requirements

12.1. Consent Documentation

All consent must be:

- written
- signed

- dated
- logged
- forwarded to the Service Manager
- stored securely under GDPR

12.2. Digital Interaction Logs

Companions must document:

- any digital assistance provided
- any recording performed
- any safeguarding concerns
- any unusual digital behaviour

13. Prohibited Actions

Companions must **never**:

- record without consent
- use client devices
- perform digital transactions
- store client data
- share client information
- use personal devices for client work
- post client content online
- engage in digital communication outside TC channels

These actions constitute **gross misconduct**.

14. 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.

15. Disciplinary Consequences

Non-compliance may result in:

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

16. Amendments

TC may update this policy to reflect:

- legal changes
- safeguarding updates
- operational improvements
- governance decisions

Updates will be communicated through official TC channels.