PRN-143: Use of Personal and Service User Devices & Digital Conduct 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 2027

---

1. Introduction

CAREHOPES is committed to ensuring the safe, lawful, professional, and appropriate use of personal devices and service user devices during companionship services.

The use of phones, tablets, laptops, smart devices, and other digital technology must never compromise safeguarding, privacy, professional boundaries, cyber security, or data protection requirements.

This policy establishes clear standards governing:

- Personal device use
- Service user device use
- Digital communication
- Recording and photography
- Cyber security
- Digital safeguarding
- Data protection and GDPR compliance
- Documentation and reporting requirements

---

2. Purpose

The purpose of this policy is to:

1. Protect service user privacy, dignity, and confidentiality.
2. Maintain appropriate professional boundaries.

3. Prevent digital abuse, exploitation, fraud, or manipulation.
4. Protect organisational and service user information.
5. Ensure compliance with UK GDPR and the Data Protection Act 2018.
6. Promote safe and responsible use of digital devices.
7. Safeguard companions from allegations, misunderstandings, or misconduct.
8. Standardise digital consent and documentation processes.
9. Reduce cyber security risks.
10. Support consistent and safe digital practice across the organisation.

---

3. Key Principles

CAREHOPES operates according to the following principles:

3.1 Safety

Device use must never compromise safeguarding or service user wellbeing.

3.2 Privacy

Service user information must remain confidential at all times.

3.3 Professionalism

Device use must support companionship activities and never distract from service delivery.

3.4 Boundaries

Personal devices must not be used in ways that blur professional relationships.

3.5 Cyber Security

All devices used for work-related purposes must comply with organisational security requirements.

3.6 Consent

Service user devices may only be accessed in accordance with this policy and with the user's permission where required.

3.7 Data Protection

All digital activities must comply with GDPR, confidentiality requirements, and organisational policies.

---

4. Scope

This policy applies to:

- Companions
- Employees
- Volunteers
- Contractors
- Agency workers
- Zero-hours workers
- Supervisors
- Managers

This policy covers:

- Personal devices
- Service user devices
- Mobile phones
- Tablets
- Laptops
- Smart watches
- Cameras
- Digital communication
- Recordings
- Data storage
- Cyber security
- Safeguarding
- Documentation

---

5. Definitions

5.1 Personal Device

Any phone, tablet, laptop, smartwatch, camera, or digital equipment owned or controlled by the worker.

5.2 Service User Device

Any phone, tablet, laptop, television, smart device, digital assistant, or other technology owned by the service user.

5.3 Digital Transaction

Any online purchase, banking activity, payment, transfer of funds, or financial operation using a digital device.

5.4 Recording

Any audio, video, photographic, screenshot, screen recording, or electronic capture of a service user, property, environment, or information.

5.5 Digital Support

Assistance provided to a service user relating to the use of technology, applications, communication tools, or online services.

---

6. Related Policies

This policy should be read alongside:

- PRN-111 Cyber Security Policy
- PRN-112 Data Protection and GDPR Policy
- PRN-102 Compliance Monitoring Policy
- PRN-109 Companionship Standards Policy
- PRN-145 Working in Pairs and Multi-Staff Working Policy
- PRN-147 Proxy Working Principle Policy
- PRN-150 Working with Vulnerable Children Policy
- Safeguarding Policy
- Confidentiality Policy
- Confidential Information Management Policy

---

7. Roles and Responsibilities

7.1 Directors and Trustees

Must:

- Oversee governance and compliance.
- Monitor policy effectiveness.
- Ensure adequate resources for safe digital practice.

7.2 Senior Management

Must:

- Approve policy updates.
- Monitor digital safeguarding risks.
- Ensure staff training is delivered.
- Review significant digital incidents.

7.3 Designated Safeguarding Lead (DSL)

Must:

- Review digital safeguarding concerns.
- Provide advice on digital risk management.
- Coordinate safeguarding responses where necessary.

7.4 Managers and Supervisors

Must:

- Monitor compliance with this policy.
- Review documentation and consent records.
- Investigate breaches and incidents.
- Support staff through training and supervision.

7.5 Staff, Volunteers and Companions

Must:

- Follow this policy at all times.
- Protect service user privacy.
- Maintain professional boundaries.
- Report concerns immediately.
- Complete accurate documentation.
- Avoid storing service user information on personal devices.

---

8. Personal Device Use

8.1 Permitted Use

Personal devices may only be used during companionship activities for:

- Accessing authorised work systems.
- Contacting management.
- Reporting safeguarding concerns.
- Completing authorised documentation.
- Emergency communication.
- Approved work-related communication.

8.2 Prohibited Use

Personal devices must not be used for:

- Personal phone calls during sessions.
- Personal conversations or messaging.
- Social media browsing.
- Personal entertainment.
- Online shopping.
- Watching videos unrelated to service delivery.
- Personal music streaming.
- Personal email relating to service user matters.
- Sharing personal contact details.
- Storing service user information.
- Proxy working.
- Shift swapping without organisational approval.

---

9. Recording and Photography

9.1 Recording Without Consent

Workers must never record a service user, property, environment, or information without appropriate consent.

Consent must be:

- Explicit
- Written
- Signed where applicable
- Dated

- Logged
- Approved where required

9.2 Acceptable Recording Purposes

Recording may only occur for:

- Safeguarding evidence.
- Documentation of damage or incidents.
- Organisationally approved records.
- Service user requested activities that have received proper consent.
- Approved communication support such as video call setup.

9.3 Prohibited Recording

Workers must not record:

- For personal use.
- For entertainment.
- For social media.
- For private storage.
- Without proper consent.

Unauthorised recording constitutes gross misconduct.

---

10. Use of Service User Devices

10.1 Guidance-First Principle

Companions should provide verbal guidance wherever possible rather than operating devices directly.

10.2 Permitted Assistance

Limited assistance may be provided when:

- The service user requests assistance.
- Permission is clearly given.
- The task is low risk.
- The task is non-clinical.
- No confidential or financial information is accessed.

Examples include:

- Assisting with making a telephone call.
- Helping access music or entertainment.
- Assisting with video call setup.
- Helping navigate simple applications.
- Supporting digital literacy and confidence.

10.3 Prohibited Access

Companions must never:

- Access emails.
- Access online banking.
- Access payment platforms.
- Access social media accounts.
- Access private messages.
- Access authentication codes.
- Store passwords.
- Create passwords.
- Manage accounts.
- Transfer files.
- Connect personal devices to service user devices.
- Contact third parties using a service user device on the user's behalf.
- Undertake care management or clinical activities.

---

11. Digital Transactions

Companions must never:

- Use service user credit or debit cards.
- Make online purchases.
- Transfer money.
- Pay bills.
- Access banking applications.
- Store card details.

- Enter PINs or passwords.
- Handle finances associated with digital transactions.

Any financial involvement may constitute gross misconduct and may result in safeguarding referrals or legal action.

---

12. Data Protection and GDPR

12.1 Prohibited Storage

Service user information must never be stored on a personal device.

This includes:

- Photographs
- Videos
- Contact details
- Passwords
- Personal documents
- Medical information
- Financial information
- Screenshots of service user data

12.2 Communication Restrictions

Staff must not:

- Share information through personal messaging applications.
- Send service user information through personal email accounts.
- Use unauthorised systems.
- Share confidential information outside approved channels.

12.3 Secure Handling

All digital information must be handled in accordance with:

- UK GDPR
- Data Protection Act 2018
- Organisational confidentiality requirements
- Data Protection and GDPR Policy
- Cyber Security Policy

---

13. Cyber Security Requirements

Workers must:

- Use strong passwords.
- Keep devices updated.
- Enable security protections.
- Lock devices when unattended.
- Use authorised systems only.
- Report cyber incidents immediately.
- Follow organisational cyber security procedures.

Workers must not:

- Disable security settings.
- Share passwords.
- Use unauthorised applications.
- Access suspicious websites or links.
- Use unsecured methods of storing service user data.
- Transfer files between personal and service user devices.

Unauthorised access may constitute both a disciplinary and safeguarding breach.

---

14. Safeguarding Requirements

Digital technology must never compromise safeguarding.

Companions must:

- Report suspicious digital activity.
- Escalate concerns of financial exploitation.
- Report cyber abuse or online manipulation.
- Maintain professional boundaries.
- Document digital risks accurately.
- Avoid involvement in service user digital disputes.
- Avoid private digital communication outside approved channels.

Where another agency or professional is already providing digital support:

- Avoid duplicating services.
- Record the involvement appropriately.
- Escalate concerns to management where necessary.

---

15. Documentation Requirements

15.1 Consent Records

All digital consent records must be:

- Written
- Dated
- Logged
- Securely stored
- Managed in accordance with GDPR requirements

15.2 Digital Interaction Records

Workers must document:

- Digital assistance provided.
- Recording activities.
- Safeguarding concerns.
- Cyber incidents.
- Unusual digital behaviour.
- External professional involvement.
- Digital risks identified.
- Actions taken.

Where another service is already providing digital support, the record should state:

"Digital support already being provided by another service."

Records must remain factual, objective, and securely stored.

---

16. Prohibited Conduct

Workers must never:

- Record without consent.
- Store service user information on personal devices.
- Share service user information inappropriately.
- Access banking systems.
- Perform digital transactions.
- Use personal devices for entertainment during sessions.
- Use devices to avoid engagement.
- Share personal contact details.
- Permit service users access to personal devices.
- Communicate privately outside approved channels.
- Conduct proxy working.
- Bypass organisational systems.
- Store passwords or login credentials.
- Transfer files between personal and service user devices.
- Post service user content online.

Any breach may constitute gross misconduct.

---

17. Legal and Regulatory Compliance

This policy aligns with:

- UK GDPR
- Data Protection Act 2018
- UK Safeguarding Legislation
- Human Rights Act 1998
- Cyber security good practice standards
- Organisational safeguarding requirements
- Organisational confidentiality requirements

All workers must comply fully with legal and organisational obligations.

---

18. Non-Compliance and Disciplinary Action

Breaches may include:

- Data breaches
- Unsafe digital behaviour
- Boundary violations
- Cyber security failures
- Safeguarding failures
- Financial misconduct
- Unauthorised recording
- Poor documentation

Consequences may include:

- Additional training
- Formal supervision
- Written warnings
- Suspension
- Removal from assignments
- Termination of engagement
- Safeguarding referral
- Regulatory notification
- Legal action where appropriate

---

19. Policy Review and Amendments

This policy shall be reviewed annually or sooner where required following:

- Legislative or regulatory changes
- Safeguarding developments
- Cyber security incidents
- Audit findings
- Organisational changes
- Governance decisions