Digital Security & Device Use Policy

PRN-44: Digital Security & Device Use 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

CAREHOPES (TC) is committed to protecting all digital information, systems, devices, and communication channels used by companions, volunteers, and staff. This Digital Security & Device Use Policy outlines:

- secure device usage
- digital confidentiality
- data protection
- communication rules
- cyber-safety
- disciplinary consequences

Digital security is a **legal obligation**, a **safeguarding requirement**, and a **core organisational priority**.

2. Purpose of the Policy

The purpose of this policy is to:

- protect confidential information
- prevent data breaches
- ensure secure device usage
- maintain safeguarding compliance
- prevent cyber-risks
- protect TC's digital infrastructure
- outline disciplinary consequences for misuse

3. Scope of the Policy

This policy applies to:

- companions
- volunteers
- permanent staff
- fixed-term staff
- contract staff
- administrators
- managers
- organisational partners (where applicable)

4. Approved Devices & Systems

4.1. TC-Approved Devices

Staff must use:

- TC-approved devices
- TC-approved software
- TC-approved communication channels

4.2. Personal Devices

Staff must **not**:

- store client information on personal devices
- store TC documents on personal devices
- use personal laptops for TC work
- use personal phones for client communication
- use personal cloud storage

This is a **confidentiality breach** and **gross misconduct**.

5. Password & Access Security

5.1. Password Requirements

Passwords must be:

- strong

- unique
- not shared
- changed regularly

5.2. Prohibited Actions

Staff must not:

- share passwords
- write passwords down in visible places
- store passwords in unsecured apps
- allow others to use their login credentials

6. Digital Confidentiality Requirements

Staff must protect:

- client information
- organisational information
- internal documents
- privileged communications
- salary and payment rate information
- mobilisation and budget structures

Strict Prohibition

Staff must **never**:

- screenshot confidential information
- forward TC emails externally
- store confidential files on personal devices
- upload TC documents to personal cloud storage
- send client information through personal messaging apps

This is **gross misconduct**.

7. Communication Security

7.1. Approved Channels

Staff must use:

- TC email
- TC messaging systems
- TC digital platforms

7.2. Prohibited Channels

Staff must not use:

- WhatsApp
- Facebook Messenger
- Instagram DM
- TikTok messages
- SMS
- personal email
- personal social media

to communicate with clients or share TC information.

8. Internet & Network Safety

Staff must:

- avoid public Wi-Fi for TC work
- avoid unsecured networks
- avoid downloading unauthorised software
- avoid clicking suspicious links
- avoid opening unknown attachments

If unsure, staff must contact TC immediately.

9. Device Security Requirements

9.1. Physical Security

Staff must:

- keep devices secure
- avoid leaving devices unattended
- lock screens when not in use
- store devices safely during travel

9.2. Digital Security

Staff must:

- install updates
- use antivirus software
- avoid unauthorised apps
- avoid storing confidential data locally

10. Social Media & Digital Conduct

Staff must:

- avoid posting confidential information
- avoid discussing TC internal matters
- avoid sharing client details
- avoid posting inappropriate content
- avoid engaging in online conflict

Staff may:

- promote TC ethically
- share referral codes
- advocate for companionship services

11. Working While on Protected Leave (Digital Restrictions)

Staff on:

- sick leave
- maternity leave
- paternity leave
- emergency leave
- compassionate leave

must **not**:

- access TC systems
- access confidential information
- perform digital work

- communicate with clients
- handle TC documents

This is **gross misconduct** and may be a **criminal offence** under UK SSP rules.

12. Digital Security During Suspension

Suspended staff must not:

- access TC systems
- access confidential information
- communicate with clients
- communicate with colleagues about the case
- post about the case online

Breaching this rule results in **immediate dismissal**.

13. Data Breach Reporting

Staff must report:

- suspicious digital activity
- unauthorised access
- lost devices
- compromised passwords
- phishing attempts
- accidental data exposure

Reports must be made **immediately** to:

admin@carehopes.com or the TC Governance & Data Protection Team.

14. Disciplinary Consequences

Digital security breaches may result in:

- written warnings
- suspension
- removal from client assignment
- summary dismissal
- safeguarding escalation

- legal referral
- ICO notification (if required)

This list is unexhausted and may be further defined by UK authorities.

15. Legal Compliance

TC complies with:

- UK GDPR
- Data Protection Act 2018
- Equality Act 2010
- ICO guidance
- UK safeguarding legislation
- international digital security standards

Breaches may result in:

- civil liability
- criminal liability
- regulatory penalties

16. Training & Awareness

TC will provide:

- digital security training
- data protection training
- device use training
- cyber-safety training

Staff must complete all mandatory training.

17. Amendments to This Policy

TC may update this policy to reflect:

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