PRN-38: Cyber Security, Information Security and Internet Fraud Awareness 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

Supersedes: PRN-173 Cyber Security and Internet Fraud Awareness Policy

---

1. Introduction

CAREHOPES is committed to maintaining the highest standards of cyber security, information security, fraud prevention, and digital safeguarding.

The organisation recognises that cybercrime, internet fraud, malicious attacks, phishing attempts, ransomware, social engineering, data breaches, and identity theft present significant risks to:

- Service users
- Staff and volunteers
- Contractors and third parties
- Organisational systems
- Financial resources
- Confidential information
- Service continuity
- Regulatory compliance
- Organisational reputation

This policy establishes the standards, responsibilities, controls, and procedures necessary to ensure secure, lawful, and resilient digital operations across all organisational activities.

---

2. Purpose

The purpose of this policy is to:

1. Protect organisational and personal information.
2. Prevent cyber attacks, internet fraud, and digital exploitation.
3. Strengthen cyber security awareness.
4. Protect service users from online scams and financial exploitation.
5. Reduce the likelihood of data breaches.
6. Promote safe digital working practices.
7. Support GDPR and information governance compliance.
8. Establish clear reporting arrangements for cyber incidents.
9. Strengthen organisational resilience and business continuity.
10. Support safeguarding through secure digital practices.

---

3. Key Principles

CAREHOPES adopts the following cyber security principles.

3.1 Confidentiality

Information must only be accessible to authorised individuals.

3.2 Integrity

Information must remain accurate, complete, and protected from unauthorised modification.

3.3 Availability

Information and systems must be available to authorised users when required.

3.4 Accountability

Every individual is personally responsible for secure use of digital systems.

3.5 Security by Design

Cyber security considerations must be embedded in all organisational systems and processes.

3.6 Risk Management

Cyber threats must be identified, assessed, monitored, and mitigated proactively.

3.7 Safeguarding

Cyber security is a safeguarding responsibility and must support the protection of vulnerable people.

3.8 Zero Tolerance

Unauthorised access, deliberate data misuse, fraud, or cyber-enabled abuse will not be tolerated.

---

4. Policy Statement

CAREHOPES will ensure that:

- Digital systems are protected against cyber threats.
- Access to information is controlled appropriately.
- Staff receive cyber security training.
- Service user information is protected.
- Cyber risks are regularly reviewed.
- Security incidents are reported and investigated.
- Digital safeguarding concerns are escalated immediately.
- Cyber security requirements align with GDPR and safeguarding obligations.
- Internet fraud risks are actively monitored and managed.

---

5. Scope

This policy applies to:

- Employees
- Companions
- Volunteers
- Contractors
- Agency workers
- Bank workers
- Students
- Trustees

- Governance personnel
- Third-party providers
- Anyone accessing organisational systems or information

This policy applies to:

- Computers
- Mobile phones
- Tablets
- Laptops
- Cloud platforms
- E-mail services
- Collaboration platforms
- Messaging systems
- Social media platforms
- Digital records
- Personal devices used for approved work
- Organisational devices
- Remote and hybrid working environments

---

6. Related Policies

- Data Protection and GDPR Policy
- Confidentiality Policy
- Confidential Information Management Policy
- Device and Digital Conduct Policy
- Information Governance Policy
- Safeguarding Adults Policy
- Safeguarding Children Policy
- Incident Reporting Policy
- Business Continuity Policy

- Proxy Working Principle Policy
- Compliance Monitoring Policy

---

7. Roles and Responsibilities

7.1 All Workers

Must:

- Follow cyber security requirements.
- Protect confidential information.
- Use approved systems appropriately.
- Maintain password security.
- Report incidents immediately.
- Complete mandatory training.
- Comply with data protection requirements.

7.2 Managers and Supervisors

Must:

- Promote cyber security awareness.
- Monitor compliance.
- Review cyber risks.
- Support investigations.
- Escalate significant concerns.
- Ensure staff training completion.

7.3 Data Protection Lead / Information Governance Lead

Must:

- Monitor compliance.
- Coordinate data breach responses.
- Support GDPR requirements.
- Maintain security records.
- Advise management during incidents.

7.4 Designated Safeguarding Lead (DSL)

Must:

- Review cyber-related safeguarding concerns.
- Coordinate safeguarding responses.
- Escalate concerns to relevant authorities.

7.5 Third-Party Providers

Must:

- Maintain appropriate cyber security measures.
- Protect confidential information.
- Report incidents promptly.
- Comply with contractual security requirements.
- Cooperate with investigations.

CAREHOPES reserves the right to review and audit compliance arrangements.

---

8. Common Cyber Threats

Workers should remain alert to:

Phishing

Fraudulent emails designed to obtain sensitive information.

Smishing

Fraudulent text message scams.

Vishing

Telephone-based scams aimed at obtaining information.

Social Engineering

Psychological manipulation to gain access to information or systems.

Identity Theft

Unauthorised use of another person's information.

Ransomware

Malicious software designed to block or encrypt systems until payment is demanded.

Malware

Software intended to damage, disrupt, or gain unauthorised access.

Business Email Compromise

Fraudulent communications appearing to originate from trusted individuals or organisations.

Internet Fraud

Any online activity designed to obtain money, information, or access through deception.

---

9. Cyber Security Standards

9.1 Device Security

All devices used for work purposes must:

- Be password protected.
- Have screen-lock functionality enabled.
- Use encryption where available.
- Have up-to-date security updates.
- Have antivirus or endpoint protection software installed where applicable.
- Be secured when unattended.
- Be used only by authorised individuals.

Lost or stolen devices must be reported immediately.

9.2 Password and Authentication Security

Workers must:

- Use strong, unique passwords.
- Use multi-factor authentication where available.
- Keep passwords confidential.
- Change passwords when compromise is suspected.
- Avoid sharing credentials.

Workers must never:

- Share passwords.
- Share authentication codes.
- Store passwords insecurely.
- Allow others to use their accounts.

9.3 Information Storage and Transmission

Information must:

- Be stored through approved systems.
- Be transmitted securely.
- Be encrypted where appropriate.
- Be accessed only on a need-to-know basis.

Workers must never:

- Send confidential information using personal email.
- Use unauthorised messaging systems.
- Store service user information on unauthorised devices.
- Transfer information to unapproved cloud services.

9.4 Internet and Online Safety

Workers must:

- Access only appropriate websites.
- Verify links before opening.
- Verify website authenticity.
- Exercise caution when downloading files.

Workers must not:

- Use unsafe websites.
- Download unauthorised software.
- Access illegal content.
- Circumvent organisational security controls.

Unsecured public Wi-Fi must not be used for organisational business unless approved security measures are in place.

9.5 Email Security

Workers must:

- Verify sender details.
- Be cautious of unexpected attachments.
- Verify unusual requests.
- Report suspicious emails immediately.
- Use organisational email systems appropriately.

Any email requesting passwords, financial information, payments, or urgent action should be treated with caution and independently verified.

9.6 Social Media Security

Workers must:

- Maintain professional boundaries.
- Protect confidentiality.
- Safeguard organisational reputation.
- Verify information before sharing.

Workers must not:

- Share confidential information.
- Discuss safeguarding matters online.
- Disclose investigations.
- Post information that compromises organisational security.
- Communicate inappropriately with service users through social media.

---

10. Protection from Internet Fraud

Workers should remain alert to:

- Fake invoices

- Impersonation scams
- Gift card scams
- Banking scams
- Investment scams
- Charity scams
- Romance scams
- Courier scams
- Remote access scams
- Payment diversion fraud

Any suspicion of fraud must be reported immediately.

No worker may provide:

- Banking details
- Authentication codes
- Financial authorisation
- Passwords
- Confidential information

to unverified individuals.

---

11. Use of Personal and Service User Devices

All workers must comply with the organisation's Device and Digital Conduct Policy.

Workers must not:

- Store service user information on personal devices.
- Connect unauthorised personal devices to organisational systems.
- Share files through unauthorised means.
- Use service user devices without authorisation.
- Transfer data between service user and personal devices.

---

12. Safeguarding and Cyber Security

Cyber security forms part of safeguarding practice.

Workers must:

- Protect service user information.
- Escalate concerns regarding cyber-enabled abuse.
- Report online exploitation concerns.
- Escalate financial exploitation concerns.
- Support safe digital inclusion.
- Maintain professional digital boundaries.

Workers must never provide financial, banking, or investment advice to service users unless explicitly authorised by their role and training.

---

13. Cyber Incident Management

13.1 Immediate Reporting

The following incidents must be reported immediately:

- Data breaches
- Cyber attacks
- Phishing attempts
- Fraud attempts
- Malware infections
- Ransomware incidents
- Password compromise
- Unauthorised access
- Lost or stolen devices

Reports must be made to management immediately.

Where safeguarding concerns exist, the DSL must also be informed.

13.2 Incident Containment

CAREHOPES may:

- Restrict accounts.
- Disable access.
- Reset passwords.
- Isolate affected systems.
- Secure information assets.
- Implement emergency controls.

13.3 Investigation

The organisation will:

- Establish root causes.
- Assess impact.
- Identify risks.
- Determine corrective actions.
- Review lessons learned.

13.4 External Notification

Where legally required, CAREHOPES may notify:

- Information Commissioner's Office (ICO)
- Police
- Local Authorities
- Safeguarding authorities
- Affected individuals
- Relevant regulators

---

14. Training Requirements

All workers must complete training in:

- Cyber Security Awareness
- GDPR and Data Protection

- Information Governance
- Digital Safeguarding
- Device Security
- Email Security
- Internet Fraud Awareness
- Incident Reporting

Training must be refreshed at least annually and more frequently where risks require.

---

15. Documentation and Record Keeping

CAREHOPES will maintain records relating to:

- Cyber incidents
- Fraud incidents
- Investigations
- Data breaches
- Corrective actions
- Security audits
- Training completion
- Device authorisations
- Access controls
- Risk assessments

Records must be:

- Accurate
- Objective
- Secure
- GDPR-compliant

---

16. Monitoring and Compliance

Compliance may be monitored through:

- Audits
- Spot checks
- Incident reviews
- Management supervision
- Quality assurance activities
- Training records
- Risk assessments
- Governance reviews

---

17. Prohibited Conduct

Workers must never:

- Share passwords.
- Share login credentials.
- Disable security controls.
- Install unauthorised software.
- Access systems without authorisation.
- Store confidential information on unauthorised devices.
- Use unauthorised cloud storage.
- Use personal messaging apps for confidential work communications.
- Conceal cyber incidents.
- Undertake proxy working.
- Share confidential information digitally without authority.
- Participate in fraud or cybercrime.
- Circumvent organisational security controls.

Serious breaches may constitute gross misconduct.

---

18. Non-Compliance

Failure to comply with this policy may result in:

- Additional training
- Corrective action plans
- Formal warnings
- Suspension
- Removal of system access
- Termination of employment or engagement
- Safeguarding referral
- Regulatory notification
- Legal action

---

19. Legal and Regulatory Compliance

This policy aligns with:

- UK GDPR
- Data Protection Act 2018
- Computer Misuse Act 1990
- Care Act 2014
- Equality Act 2010
- Human Rights Act 1998
- ICO guidance
- UK cyber security good practice standards
- Organisational safeguarding requirements

---

20. Policy Review

This policy will be reviewed annually or sooner following:

- Significant cyber incidents
- Legislative changes
- Regulatory changes
- Technological developments

- Audit findings
- Organisational changes
- Emerging cyber threats