Cyber Security Policy

PRN-38: Cyber Security 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. Policy Introduction

Trusted Companionship, the trading name of AI Auto-Tech Ltd, is committed to maintaining the highest standards of cyber security to protect service users, staff, organisational data, digital systems, and operational integrity. Cyber security is essential for safeguarding sensitive information, preventing data breaches, ensuring regulatory compliance, and maintaining trust.

This policy outlines the organisation's cyber security standards, responsibilities, and procedures to ensure safe, lawful, and secure digital operations.

2. Key Principles

- **Confidentiality:** Protect all personal, organisational, and sensitive data.
- **Integrity:** Ensure information is accurate, complete, and protected from unauthorised modification.
- **Availability:** Ensure systems and data are accessible to authorised users when required.
- **Compliance:** Adhere to GDPR, UK data protection laws, and organisational policies.
- **Risk Management:** Identify, assess, and mitigate cyber risks proactively.
- **Accountability:** All staff share responsibility for cyber security.
- **Zero Tolerance:** No unauthorised access, sharing, or misuse of digital systems.

3. Policy Statement

Trusted Companionship ensures that:

- All digital systems are protected against cyber threats
- Staff follow cyber security protocols and GDPR requirements
- Devices are used safely and appropriately
- Data is stored, transmitted, and accessed securely
- Cyber incidents are reported immediately
- Staff receive cyber security training
- Access to systems is strictly controlled
- Digital behaviour aligns with safeguarding and organisational standards

4. Purpose

- Protect organisational and personal data
- Prevent cyber attacks, breaches, and misuse
- Ensure compliance with legal and regulatory requirements
- Provide clear guidance for digital safety
- Strengthen organisational resilience
- Support safe digital operations across all environments

5. Scope

This policy applies to:

- All employees
- Volunteers
- Contractors
- Agency workers
- Zero-contract workers (**PRN-149**)
- Trustees and governance personnel

It covers:

- Digital systems
- Devices

- Data storage
- Data transmission
- Online behaviour
- Cyber incident response
- Password security
- Access control
- Use of personal and service user gadgets (**PRN-148**)

6. Related Policies

PRN-112 Data Protection and GDPR Policy PRN-148 Use of Personal and Service Users Gadget Policy PRN-102 Compliance Monitoring PRN-104 Policy Review PRN-109 Companionship Standards Policy PRN-145 Working in Pairs and Multi-Staff Working Policy PRN-147 Proxy Working Principle PRN-150 Working with Vulnerable Children Policy

7. Cyber Security Standards

7.1 Device Security

All devices used for work must:

- Have password protection
- Use encrypted storage
- Have up-to-date antivirus software
- Be locked when unattended
- Be used only by authorised staff

Personal devices must **not** store or transmit service user data unless authorised under PRN-148.

7.2 Password and Access Control

Staff must:

- Use strong passwords
- Change passwords regularly
- Never share passwords
- Never write passwords down

- Use multi-factor authentication where required
- Access only systems relevant to their role

Unauthorised access is a disciplinary and safeguarding breach.

7.3 Data Storage and Transmission

Data must:

- Be stored securely
- Be transmitted only through approved channels
- Never be sent via personal email or messaging apps
- Never be stored on unauthorised devices
- Be encrypted when required

Service user data must never be stored on personal gadgets unless authorised under PRN-148.

7.4 Safe Internet Use

Staff must:

- Avoid unsafe websites
- Avoid downloading unauthorised files
- Avoid clicking suspicious links
- Avoid using public Wi-Fi for work unless using secure VPN
- Maintain professional digital behaviour

7.5 Email Security

Staff must:

- Verify sender identity
- Avoid opening suspicious attachments
- Avoid responding to phishing attempts
- Report suspicious emails immediately
- Use work email only for authorised communication

7.6 Use of Personal and Service User Gadgets

Staff must follow PRN-148, including:

- No unauthorised use of service user devices
- No storing service user data on personal devices
- No connecting personal devices to service user networks
- No sharing files between personal and work devices

8. Safeguarding and Cyber Security

Cyber security is a safeguarding requirement.

Staff must:

- Protect service user information
- Avoid digital contact with children
- Avoid sharing personal contact details
- Report digital safeguarding concerns immediately
- Document digital risks accurately

Digital behaviour must align with PRN-143 and PRN-150.

9. Cyber Incident Response

9.1 Report Immediately

Staff must report:

- Data breaches
- Suspicious activity
- Phishing attempts
- Malware infections
- Unauthorised access
- Lost or stolen devices

Reports must be made to:

- Senior management
- Data Protection Officer
- DSL (if safeguarding-related)

9.2 Containment

Management will:

- Secure affected systems
- Change passwords
- Restrict access
- Notify relevant authorities if required

9.3 Investigation

Incidents will be investigated to:

- Identify cause
- Assess impact
- Prevent recurrence

9.4 Notification

If required, the organisation will notify:

- ICO (Information Commissioner's Office)
- Affected individuals
- Safeguarding authorities

10. Prohibited Conduct

Staff must **not**:

- Share passwords
- Access unauthorised systems
- Store data on personal devices
- Use service user gadgets without permission
- Disable security settings
- Install unauthorised software
- Engage in proxy working
- Swap shifts without TC approval
- Share confidential information digitally
- Use personal messaging apps for work

11. Training Requirements

Staff must receive training in:

- Cyber security
- GDPR and data protection
- Digital safeguarding
- Device safety
- Email security
- Incident reporting

Training must be refreshed annually.

12. Documentation Requirements

Records must include:

- Cyber incidents
- Investigations
- Corrective actions
- Training completion
- Access control logs
- Device authorisations

All records must be factual, objective, and securely stored.

13. Non-Compliance

Non-compliance may include:

- Data breaches
- Unsafe digital behaviour
- Password sharing
- Proxy working
- Poor documentation
- Safeguarding failures

Consequences may include:

- Retraining
- Formal warnings
- Suspension

- Termination
- Referral to safeguarding authorities
- Legal action

14. Policy Review

This policy will be reviewed annually or sooner if required due to:

- Legislative changes
- Cyber security developments
- Organisational changes
- Audit findings

Next Review Date: (Month and Year)