INFORMATION GOVERNANCE AND CYBER SECURITY POLICY

PRN-80: Information Governance and 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. Purpose

The purpose of this policy is to establish the organisation's approach to information governance, cyber security, and the protection of information assets.

The organisation recognises that information is a valuable asset and that effective information governance is essential for:

- Protecting confidential information.
- Maintaining service user trust.
- Supporting safe service delivery.
- Complying with legal obligations.
- Preventing data breaches.
- Reducing cyber security risks.
- Ensuring business continuity.

As a Non-Accommodation Companionship and Wellbeing Support Service supporting older people and adults with disabilities, the organisation is committed to ensuring that information is managed securely, lawfully, and responsibly.

---

2. Scope

This policy applies to:

- Employees
- Volunteers

- Managers
- Directors
- Trustees
- Contractors
- Agency workers
- Students and placements

The policy applies to:

- Electronic information
- Paper records
- Emails
- Mobile devices
- Cloud-based systems
- Digital communications
- Organisational websites
- Social media accounts
- Information systems

---

3. Policy Statement

The organisation is committed to:

- Protecting information assets.
- Promoting information security awareness.
- Preventing cyber incidents.
- Responding effectively to security breaches.
- Maintaining confidentiality, integrity, and availability of information.
- Complying with relevant legislation and best practice.

Information security is everyone's responsibility.

---

4. Objectives

The objectives of this policy are to:

- Protect personal and confidential information.
- Safeguard organisational systems.
- Reduce cyber security risks.
- Promote responsible use of technology.
- Ensure resilience against cyber threats.
- Support legal compliance.
- Protect organisational reputation.

---

5. Legal and Regulatory Framework

This policy is informed by:

- UK GDPR
- Data Protection Act 2018
- Computer Misuse Act 1990
- Human Rights Act 1998
- Privacy and Electronic Communications Regulations (PECR)
- Common Law Duty of Confidentiality

The organisation will comply with applicable information governance and data protection requirements.

---

6. Information Governance Principles

The organisation will ensure information is:

Confidential

Protected from unauthorised access.

Accurate

Reliable, current, and maintained appropriately.

Available

Accessible to authorised individuals when required.

Secure

Protected against loss, alteration, disclosure, or destruction.

Accountable

Managed in accordance with organisational procedures.

---

7. Information Assets

Information assets may include:

- Service user records
- Volunteer records
- Employee records
- Financial information
- Safeguarding records
- Email communications
- Policies and procedures
- Digital databases
- Cloud storage systems
- Training records

All information assets should be protected appropriately.

---

8. Cyber Security Principles

The organisation will promote:

Prevention

Preventing security incidents where possible.

Protection

Protecting systems and information.

Detection

Identifying threats promptly.

Response

Responding effectively to incidents.

Recovery

Restoring services and information following incidents.

---

9. Access Control

Access to information should be restricted to authorised individuals.

Controls may include:

- User accounts.
- Password protection.
- Access permissions.
- Role-based access arrangements.
- Multi-factor authentication where available.

Access rights should be reviewed regularly.

---

10. Password Security

All users must maintain strong password practices.

Passwords should:

- Be unique.
- Be difficult to guess.
- Not be shared with others.
- Be changed if compromise is suspected.

Individuals must not:

- Share passwords.
- Write passwords in insecure locations.
- Use another person's login credentials.

---

11. Multi-Factor Authentication

Where systems support multi-factor authentication (MFA), users should enable and utilise it.

MFA provides an additional layer of protection against unauthorised access.

---

12. Email Security

Users must exercise caution when using email.

Employees and volunteers should:

- Verify recipients before sending information.
- Avoid opening suspicious attachments.
- Report suspicious emails.
- Use authorised organisational email accounts where available.

Sensitive information should only be shared appropriately and securely.

---

13. Phishing and Social Engineering

Cyber criminals may attempt to obtain information through deception.

Examples include:

- Phishing emails.
- Fraudulent text messages.
- Telephone scams.
- Impersonation attempts.

Employees and volunteers should:

- Remain vigilant.
- Verify requests.
- Report suspicious communications immediately.

---

14. Malware and Viruses

Users should not:

- Download unauthorised software.

- Open suspicious files.
- Bypass security protections.

Appropriate anti-virus and security measures should be maintained on organisational systems where applicable.

---

15. Use of Organisational Devices

Organisational devices should be used responsibly.

Users must:

- Protect devices from theft or loss.
- Lock devices when unattended.
- Install updates when required.
- Follow organisational IT requirements.

Devices remain organisational property unless otherwise stated.

---

16. Personal Devices

Where personal devices are used for organisational activities:

- Management approval should be obtained where required.
- Data protection obligations must be followed.
- Appropriate security controls should be used.

Personal devices should not compromise information security.

---

17. Home and Remote Working

Employees and volunteers working remotely must:

- Protect confidential information.
- Secure devices appropriately.
- Avoid public access to sensitive information.
- Use secure internet connections where possible.

Remote working arrangements should support safe handling of information.

---

18. Data Storage

Information should only be stored in approved locations.

Storage arrangements should:

- Protect confidentiality.
- Prevent unauthorised access.
- Support business continuity.
- Enable appropriate backup arrangements.

Users should avoid storing organisational data in unauthorised locations.

---

19. Backups and Data Recovery

Where appropriate, systems and information should be backed up regularly.

Backup arrangements should:

- Support recovery following incidents.
- Protect against data loss.
- Be tested periodically where possible.

---

20. Software Updates and Patch Management

Systems should be maintained with appropriate updates.

Updates help protect against:

- Security vulnerabilities.
- Malware attacks.
- Cyber security threats.

Users should not intentionally disable security updates.

---

21. Secure Disposal of Information and Equipment

Information and equipment must be disposed of securely.

Examples include:

Paper Information

- Confidential shredding.

Electronic Information

- Secure deletion.
- Data wiping procedures.

Equipment

- Removal of stored data prior to disposal.

Disposal arrangements must protect confidential information.

---

22. Cyber Security Incident Reporting

Cyber security incidents may include:

- Hacking attempts.
- Malware infections.
- Lost devices.
- Data breaches.
- Unauthorised access.
- Phishing attacks.

All suspected incidents must be reported immediately.

---

23. Responding to Cyber Incidents

Where a cyber incident occurs:

Step 1

Report the incident immediately.

Step 2

Contain the threat where possible.

Step 3

Notify management.

Step 4

Assess the impact.

Step 5

Implement corrective actions.

Step 6

Document the incident and learning outcomes.

---

24. Data Breaches

A data breach may involve:

- Loss of personal information.
- Unauthorised disclosure.
- Accidental sharing.
- Theft of records.
- Unauthorised access.

All data breaches must be reported immediately in accordance with organisational procedures.

---

25. Business Continuity and Cyber Resilience

Cyber security arrangements should support business continuity planning.

The organisation will seek to:

- Maintain critical services.
- Recover information when possible.
- Reduce disruption.
- Learn from incidents.

Resilience planning supports operational continuity.

---

26. Information Sharing and Confidentiality

Information sharing must comply with:

- Confidentiality requirements.

- Data protection legislation.
- Organisational procedures.

Information should only be shared:

- Where necessary.
- With authorised persons.
- For legitimate purposes.

---

27. Training and Awareness

Employees and volunteers will receive training relevant to their role covering:

- Data protection.
- Information governance.
- Cyber security awareness.
- Password security.
- Phishing awareness.
- Incident reporting.

Awareness training should be refreshed periodically.

---

28. Third-Party Providers

Where third-party systems or providers are used:

- Appropriate due diligence should be undertaken.
- Security arrangements should be considered.
- Data processing requirements should be addressed where applicable.

The organisation remains accountable for information handled on its behalf.

---

29. Monitoring and Audit

The organisation may monitor:

- Information security incidents.
- Data breaches.

- System access arrangements.
- Cyber security risks.
- Training compliance.
- Audit outcomes.

Monitoring helps identify improvements and reduce risks.

---

30. Responsibilities

Board of Trustees

Responsible for:

- Strategic oversight.
- Information governance leadership.
- Monitoring cyber security risks.

Directors

Responsible for:

- Implementing this policy.
- Managing cyber security risks.
- Ensuring incident response arrangements are in place.

Managers

Responsible for:

- Supporting compliance.
- Reporting incidents.
- Promoting information security awareness.

Employees and Volunteers

Responsible for:

- Protecting information.
- Following security procedures.
- Reporting incidents promptly.
- Completing required training.

---

31. Case Study

Scenario: Suspicious Email Received

A volunteer receives an email claiming to be from a bank requesting account details.

Action Taken

- The volunteer does not click any links.
- The email is reported to management.
- The message is deleted after review.

Outcome

A potential phishing attack is avoided and awareness is reinforced.

Learning Point

Vigilance and prompt reporting are essential components of cyber security.

---

32. Monitoring and Quality Assurance

The organisation will monitor:

- Information governance compliance.
- Cyber security incidents.
- Data breaches.
- Training completion.
- Access control arrangements.
- Audit findings.
- Lessons learned from incidents.

Findings will be used to improve information security and organisational resilience.

---

33. Review Arrangements

This policy will be reviewed:

- Annually.

- Following cyber security incidents.
- Following significant data breaches.
- Following legislative or regulatory changes.
- Following organisational or technological changes.

Related Policies

- Data Protection and GDPR Policy
- Confidentiality Policy
- Records Management and Record Keeping Policy
- Information Sharing and Confidentiality Procedure
- Business Continuity and Emergency Planning Policy
- Risk Assessment Policy
- Employee Use of Technology and Social Media Policy
- Incident Reporting Policy