Confidential Information Management Policy

PRN-31: **Confidential Information Management 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 confidential information relating to:

- clients
- companions
- volunteers
- staff
- organisational operations
- financial structures
- internal documents
- privileged communications

This Confidential Information Management Policy outlines how staff must handle, store, share, and protect confidential information in compliance with:

- UK GDPR
- Data Protection Act 2018
- Equality Act 2010
- UK safeguarding standards
- TC governance and disciplinary rules

Confidentiality is a **core safeguarding requirement** and a **legal obligation**.

2. Purpose of the Policy

The purpose of this policy is to:

- define confidential information
- outline staff responsibilities
- prevent unauthorised disclosure
- protect client privacy
- protect organisational integrity
- ensure legal compliance
- prevent misuse of sensitive information
- outline disciplinary and criminal consequences

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. Definition of Confidential Information

Confidential information includes, but is not limited to:

4.1. Client Information

- names
- addresses
- medical conditions
- care plans
- behavioural notes
- vulnerabilities
- personal preferences

- financial information
- family details

4.2. Staff Information

- salary
- payment rate
- personal details
- disciplinary records
- performance records
- internal communications

4.3. Organisational Information

- TC budget distribution
- mobilisation cost structure
- internal policies
- operational procedures
- financial models
- referral systems
- privileged internal communications

4.4. Documents & Files

- digital files
- printed documents
- client notes
- internal reports
- investigation records
- HR documents

4.5. Privileged Information

- legal advice
- board communications
- safeguarding reports

- investigation findings

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

5. Strict Prohibition: Salary & Payment Rate Disclosure

5.1. Salary Negotiation Clause

All staff negotiate their salary **before engagement**. Salary information is **private, confidential, and protected** under TC's Data Policy.

5.2. Prohibited Actions

Staff must **never**, under any circumstance:

- disclose their salary
- disclose their payment rate
- compare rates with clients
- discuss how much TC pays them
- explain TC's budget distribution
- reveal mobilisation cost structure
- discuss internal financial allocations

5.3. Classification of Breach

Salary disclosure is:

- **Gross Misconduct**
- a **breach of confidentiality**
- a **breach of UK GDPR**
- a **breach of Data Protection Act 2018**
- **misrepresentation**
- grounds for **summary dismissal**

5.4. Reason for Prohibition

Clients and staff **do not understand**:

- TC's budget portfolio
- operational costs
- mobilisation compositions

- safeguarding overheads
- insurance and compliance costs
- administrative infrastructure

Disclosure creates:

- false expectations
- financial conflict
- reputational damage
- safeguarding risk

6. Client Confidentiality Requirements

Staff must protect all client information and must not:

- share client details with third parties
- discuss client cases publicly
- post client information online
- store client data on personal devices
- disclose client vulnerabilities
- share client photos or videos
- discuss client behaviour outside TC channels

Breaching client confidentiality is:

- **Gross Misconduct**
- a **safeguarding violation**
- grounds for **immediate dismissal**
- grounds for **legal escalation**

7. Organisational Confidentiality Requirements

Staff must not disclose:

- internal policies
- operational procedures
- financial structures
- mobilisation processes

- referral systems
- internal communications
- investigation details
- disciplinary outcomes
- privileged information

This includes:

- verbal disclosure
- written disclosure
- digital disclosure
- social media disclosure

8. Document & File Management

8.1. Storage

Staff must:

- store documents securely
- use TC-approved systems
- avoid personal devices
- avoid unencrypted storage

8.2. Transmission

Staff must not:

- email confidential documents externally
- use personal email accounts
- use unauthorised cloud storage
- share files via social media

8.3. Disposal

Confidential documents must be:

- shredded
- securely deleted
- disposed of according to TC procedures

9. Digital Confidentiality Requirements

Staff must:

- use TC-approved devices
- use secure passwords
- avoid public Wi-Fi for confidential work
- avoid screenshots of confidential data
- avoid storing client information on phones
- avoid forwarding TC emails externally

10. Working While on Sick or Protected Leave (Confidentiality Risk)

Staff on:

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

must **not**:

- access confidential information
- engage in TC work
- handle client data
- perform administrative duties

Doing so is:

- **Gross Misconduct**
- a **criminal offence** under UK SSP rules
- grounds for **summary dismissal**

11. Confidentiality During Suspension or Investigation

Staff under suspension or investigation must not:

- discuss the case
- contact clients

- contact colleagues about the case
- disclose investigation details
- share internal documents
- post about the case online

Breaching confidentiality during suspension is grounds for **immediate dismissal**.

12. Resignation While Confidentiality Investigation Is Ongoing

If staff resign during a confidentiality-related investigation:

12.1. Investigation Continues

TC will:

- continue the investigation
- document findings
- escalate safeguarding concerns
- notify external authorities (if required)

12.2. Reference Impact

References will be:

- factual only
- not character-based
- not performance-based

TC will disclose:

- dates of employment
- job title
- resignation during investigation
- safeguarding concerns (if legally required)

12.3. Re-Employment Eligibility

Staff who resign during a confidentiality investigation:

- are **not eligible** for re-employment
- may be permanently barred
- may be flagged in safeguarding records

13. Disciplinary Consequences for Confidentiality Breaches

Breaches may result in:

- informal warning
- written warning
- final warning
- suspension
- removal from client assignment
- summary dismissal
- legal escalation
- safeguarding referral
- police involvement (if criminal)

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

14. Legal & Regulatory Compliance

TC complies with:

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

Breaches may result in:

- civil liability
- criminal liability
- regulatory penalties

15. Staff Training & Awareness

TC will provide:

- confidentiality training
- safeguarding training

- data protection training
- digital security training

Staff must complete all mandatory training.

16. Amendments to This Policy

TC may update this policy to reflect:

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

Updates will be communicated through official TC channels.