Data Protection and GDPR Policy

PRN-40: Data Protection and GDPR 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. Policy Introduction

CAREHOPES, the trading name of AI Auto-Tech Ltd, is committed to protecting all personal, sensitive, and confidential information relating to service users, staff, external professionals, and organisational operations. This policy ensures full compliance with:

- UK GDPR
- Data Protection Act 2018
- ICO guidance
- Organisational safeguarding and cyber-security standards

Data protection is a legal, ethical, and safeguarding requirement. Every staff member plays a critical role in maintaining confidentiality, security, and lawful data handling.

2. Key Principles

- **Lawfulness:** All data processing must comply with UK GDPR and UK law.
- **Fairness:** Data must be handled transparently and ethically.
- **Purpose Limitation:** Data must only be used for legitimate organisational purposes.
- **Data Minimisation:** Only essential data is collected and processed.
- **Accuracy:** Data must be kept accurate and up-to-date.
- **Storage Limitation:** Data must not be kept longer than necessary.
- **Integrity & Confidentiality:** Data must be protected against unauthorised access, loss, or damage.
- **Accountability:** CAREHOPES must demonstrate compliance at all times.

3. Policy Statement

CAREHOPES ensures that:

- All personal data is processed lawfully and securely
- Staff follow strict confidentiality and data protection rules
- Digital systems comply with cyber-security standards (PRN-111)
- Service user information is protected at all times
- Data breaches are reported immediately
- Staff receive mandatory GDPR training
- Personal devices are not used for data storage unless authorised
- Service user gadgets are handled according to PRN-148
- Safeguarding requirements override data restrictions when necessary

4. Purpose

- Protect personal and sensitive information
- Ensure compliance with UK GDPR and Data Protection Act 2018
- Prevent data breaches and misuse
- Provide clear guidance for staff
- Strengthen organisational safeguarding and cyber-security
- Maintain trust with service users, staff, and external partners

5. Scope

This policy applies to:

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

It covers:

- Data collection
- Data storage

- Data transmission
- Data access
- Data deletion
- Digital systems
- Paper records
- Cyber-security
- Safeguarding information
- Use of personal and service user gadgets (**PRN-148**)

6. Related Policies

PRN-111 Cyber Security 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. Types of Data Covered

7.1 Personal Data

Includes:

- Name
- Address
- Contact details
- Date of birth
- Gender

7.2 Special Category Data

Includes:

- Health information
- Safeguarding information
- Cultural or religious data
- Sexual orientation
- Gender identity

- Disability information

7.3 Staff Data

Includes:

- DBS status
- Training records
- Employment information
- Allocation restrictions
- Disciplinary history

7.4 Digital Data

Includes:

- Emails
- Digital notes
- System logs
- Device data
- Online communications

8. Lawful Bases for Processing

CAREHOPES processes data under:

- **Consent**
- **Contractual necessity**
- **Legal obligation**
- **Vital interests**
- **Public interest**
- **Legitimate interest**

Safeguarding concerns may override consent when necessary to protect a vulnerable person.

9. Data Collection Standards

Data must be:

- Relevant

- Necessary
- Collected lawfully
- Collected transparently
- Documented accurately

Service users must be informed about:

- What data is collected
- Why it is collected
- How it is stored
- Who it is shared with
- Their rights under GDPR

10. Data Storage Standards

Data must be stored:

- Securely
- Encrypted where required
- On authorised systems only
- With restricted access
- In line with cyber-security protocols

Paper records must be:

- Locked away
- Accessed only by authorised staff
- Shredded when no longer needed

11. Data Transmission Standards

Data must **not** be transmitted via:

- Personal email
- Personal messaging apps
- Social media
- Unsecured networks
- Service user devices

Data must be transmitted only through:

- Approved organisational systems
- Encrypted channels
- Secure digital platforms

12. Use of Personal and Service User Gadgets (PRN-148)

Staff must:

- Never store service user data on personal devices
- Never use service user gadgets to access organisational systems
- Never transfer files between personal and work devices
- Follow PRN-148 at all times

13. Access Control

Access must be:

- Role-based
- Logged
- Monitored
- Revoked when no longer required

Unauthorised access is a disciplinary and safeguarding breach.

14. Data Sharing

Data may be shared with:

- Safeguarding authorities
- Police
- Social workers
- Health professionals
- Regulatory bodies

Data must **not** be shared with:

- Friends
- Family members
- Unauthorised staff

- External individuals without legal basis

15. Data Breach Procedure

15.1 Immediate Reporting

Staff must report:

- Lost devices
- Unauthorised access
- Suspicious digital activity
- Accidental data disclosure
- Cyber incidents

Reports must be made to:

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

15.2 Containment

Management will:

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

15.3 Investigation

Investigations will:

- Identify cause
- Assess impact
- Prevent recurrence

15.4 Notification

If required, the organisation will notify:

- ICO
- Affected individuals

- Safeguarding authorities

16. Rights of Service Users

Service users have the right to:

- Access their data
- Request corrections
- Request deletion (where lawful)
- Restrict processing
- Object to processing
- Data portability
- Withdraw consent

Requests must be processed within legal timeframes.

17. Training Requirements

Staff must receive training in:

- GDPR
- Data protection
- Cyber security
- Digital safeguarding
- Device safety
- Incident reporting

Training must be refreshed annually.

18. Documentation Requirements

Records must include:

- Data breaches
- Investigations
- Corrective actions
- Training completion
- Access logs
- Consent records

- Privacy notices

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

19. 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

20. Policy Review

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

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