INFORMATION SHARING AND CONFIDENTIALITY PROCEDURE

PRN-81: Information Sharing and Confidentiality Procedure

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. Purpose

This procedure provides practical guidance on the safe handling, sharing, storage, and protection of information relating to service users, employees, volunteers, and other stakeholders.

The organisation recognises that confidentiality is fundamental to building trust, protecting privacy, and maintaining professional standards.

This procedure aims to:

- Protect confidential information.
- Ensure lawful information sharing.
- Support safeguarding responsibilities.
- Promote consistent record keeping.
- Ensure compliance with Data Protection legislation.
- Protect the rights and dignity of individuals.

---

2. Scope

This procedure applies to:

- Employees
- Volunteers
- Managers

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

The procedure applies to:

- Paper records
- Electronic records
- Emails
- Verbal communication
- Text messages
- Photographs
- Meeting notes
- Reports
- Personal information

---

3. Key Principles

All information must be handled in accordance with the following principles:

Respect

Individuals have a right to privacy.

Necessity

Only information that is necessary should be collected or shared.

Confidentiality

Information should only be accessed by authorised individuals.

Security

Information must be protected against loss, theft, or unauthorised access.

Accountability

Individuals are responsible for handling information appropriately.

---

4. What is Confidential Information?

Confidential information is any information that is not publicly available and relates to an identifiable individual or organisation.

Examples include:

- Personal details
- Contact information
- Health information
- Support plans
- Safeguarding records
- Financial information
- Employment records
- Volunteer records
- Complaints information

Confidential information must be treated with care and respect.

---

5. Responsibilities

Managers

Responsible for:

- Providing guidance.
- Supporting compliance.
- Managing breaches appropriately.
- Monitoring record keeping and information sharing.

Employees and Volunteers

Responsible for:

- Maintaining confidentiality.
- Following this procedure.
- Protecting information.

- Reporting concerns or breaches.

Directors

Responsible for:

- Governance oversight.
- Ensuring appropriate systems are in place.
- Monitoring compliance with data protection requirements.

---

6. Collecting Information

Only information necessary for legitimate organisational purposes should be collected.

Information collected should be:

- Relevant.
- Accurate.
- Up to date.
- Necessary for service delivery or organisational functions.

Individuals should be informed about how their information will be used.

---

7. Accessing Information

Employees and volunteers should only access information that they require to perform their role.

Individuals must not:

- Access records out of curiosity.
- Access records without authorisation.
- Share information inappropriately.

Access should always be on a need-to-know basis.

---

8. Obtaining Consent for Information Sharing

Where appropriate, consent should be obtained before information is shared.

Employees and volunteers should explain:

- What information will be shared.
- Why it is being shared.
- Who it will be shared with.
- Potential benefits of sharing.

Consent should be recorded where appropriate.

---

9. Information Sharing with Service User Consent

Information may be shared where:

- Consent has been given.
- Sharing supports the individual's wellbeing.
- Sharing supports service delivery.
- Sharing promotes positive outcomes.

Examples may include:

- Referrals to community services.
- Communication with healthcare professionals.
- Support planning discussions.

---

10. Sharing Information Without Consent

Information may be shared without consent where:

- A safeguarding concern exists.
- Serious harm may occur.
- A crime may have been committed.
- There is a legal requirement to disclose information.
- Public protection concerns exist.

Any decision to share information without consent should be:

- Necessary.
- Proportionate.
- Justifiable.

- Properly recorded.

---

11. Safeguarding and Information Sharing

Safeguarding concerns take priority over confidentiality where individuals may be at risk.

Employees and volunteers should:

- Report safeguarding concerns promptly.
- Share relevant information with safeguarding professionals.
- Follow safeguarding procedures.

Confidentiality must never prevent appropriate safeguarding action.

---

12. Verbal Information Sharing

Confidential information should only be discussed:

- In appropriate settings.
- With authorised individuals.
- For legitimate organisational purposes.

Employees and volunteers should avoid discussing confidential matters:

- In public places.
- On public transport.
- In social settings.
- Within hearing distance of unauthorised persons.

---

13. Email Communication

When sending emails containing personal information:

Employees and volunteers should:

- Use authorised systems.
- Check recipient details carefully.
- Share only necessary information.

- Use secure attachments where appropriate.

Care should be taken to avoid accidental disclosure.

---

14. Telephone Communication

Before discussing confidential information by telephone:

- Confirm the identity of the caller.
- Ensure they are authorised to receive information.
- Share only the information required.

Where identity cannot be verified, information should not be disclosed.

---

15. Electronic Records

Electronic records must be:

- Password protected.
- Access restricted.
- Securely stored.
- Regularly backed up where appropriate.

Devices containing confidential information should not be left unattended.

---

16. Paper Records

Paper records should be:

- Stored securely.
- Kept in locked facilities where appropriate.
- Protected from damage and loss.
- Accessible only to authorised individuals.

Confidential records should never be left unattended in public areas.

---

17. Working Remotely

Employees and volunteers undertaking remote work must:

- Protect confidential information.
- Secure devices appropriately.
- Avoid public viewing of records.
- Follow organisational data protection requirements.

Extra care should be taken when handling sensitive information away from organisational premises.

---

18. Photographs, Video and Recordings

Photographs, video recordings, or audio recordings should only be taken where:

- Appropriate consent has been obtained.
- There is a legitimate organisational purpose.
- Storage arrangements are secure.

Images and recordings must not be shared without appropriate authorisation.

---

19. Information Sharing with Family Members

Information should only be shared with family members where:

- Consent exists; or
- A lawful basis allows sharing.

Employees and volunteers must not assume that family members automatically have a right to information.

The service user's wishes should be considered wherever possible.

---

20. Requests for Information

If a request is received from:

- Police
- Local Authority
- NHS Professional
- Solicitor
- Regulatory Body

Employees and volunteers should refer the request to their manager unless established procedures apply.

All requests should be handled appropriately and documented where necessary.

---

21. Data Breaches

Examples of information breaches include:

- Lost records.
- Misdirected emails.
- Unauthorised disclosure.
- Stolen devices.
- Records viewed by unauthorised persons.

All suspected breaches must be reported immediately to management.

---

22. Responding to a Data Breach

Step 1

Report the breach immediately.

Step 2

Contain the breach where possible.

Step 3

Inform management.

Step 4

Assess the risk.

Step 5

Implement corrective action.

Step 6

Record and investigate the incident.

---

23. Record Keeping

Records relating to information sharing should include:

- Date.
- Information shared.
- Person receiving information.
- Purpose of sharing.
- Consent obtained (where applicable).
- Reason for sharing without consent (where applicable).

Accurate records promote accountability and transparency.

---

24. Confidentiality Breaches

Examples include:

- Gossiping about service users.
- Discussing confidential information in public.
- Accessing records without authorisation.
- Sharing information through personal devices.
- Disclosing information unnecessarily.

Breaches may result in disciplinary or management action.

---

25. Information Sharing Decision-Making Flowchart

Information Identified

↓

Is Sharing Necessary?

↓

No → Do Not Share

Yes

↓

Consent Available?

↓

Yes → Share Appropriately → Record Action

No

↓

Safeguarding Risk / Legal Basis Exists?

↓

No → Do Not Share

Yes → Share Relevant Information → Record Reason

↓

Review Outcome

---

26. Case Study

Scenario: Possible Safeguarding Concern

A volunteer becomes concerned that a service user is experiencing financial abuse and wishes to share information with the Designated Safeguarding Lead.

Action Taken

- The volunteer records concerns factually.
- Relevant information is shared promptly with the Designated Safeguarding Lead.
- The reason for sharing without consent is documented.
- Safeguarding procedures are followed.

Outcome

The concern is assessed and referred appropriately.

Learning Point

Confidentiality should never prevent information sharing where an individual may be at risk of harm.

---

27. Training Requirements

Employees and volunteers will receive training appropriate to their role in:

- Confidentiality
- Data Protection and GDPR

- Safeguarding
- Information Sharing
- Record Keeping
- Cyber Security Awareness

Training compliance will be monitored and reviewed.

---

28. Monitoring and Quality Assurance

The organisation will monitor:

- Information sharing practices.
- Confidentiality breaches.
- Data breaches.
- Training compliance.
- Audit findings.
- Service user concerns relating to confidentiality.

Monitoring findings will be used to improve information governance arrangements.

---

29. Responsibilities Summary

Role	Key Responsibilities
Directors	Governance oversight and legal compliance
Managers	Advice, monitoring, breach management
Employees	Confidential handling of information
Volunteers	Protecting information and reporting concerns

---

30. Review Arrangements

This procedure will be reviewed:

- Annually.

- Following data breaches.
- Following legislative changes.
- Following safeguarding reviews.
- Following significant organisational changes.

Related Policies

- Confidentiality Policy
- Data Protection and GDPR Policy
- Adult Safeguarding Policy
- Records Management and Record Keeping Policy
- Information Governance Policy
- Service User Consent and Capacity Procedure
- Complaints Policy
- Whistleblowing Policy