SERVICE USER CONFIDENTIALITY AND CONSENT PROCEDURE

PRN-121: Service User Confidentiality and Consent 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 guidance on obtaining, recording, reviewing, and managing consent while ensuring the confidentiality of service user information.

The organisation recognises that confidentiality and consent are fundamental to building trust, promoting dignity, respecting individual rights, and ensuring compliance with legal and professional responsibilities.

This procedure aims to:

Protect service user information.

Support informed decision-making.

Ensure lawful information sharing.

Promote person-centred practice.

Maintain trust and confidence.

Support safeguarding and wellbeing.

---

2. Scope

This procedure applies to:

Employees

Volunteers

Managers

Directors

Trustees where relevant

Contractors acting on behalf of the organisation

It applies to all personal information obtained, stored, used, shared, and managed during service delivery.

---

3. Principles

The organisation will ensure that information is managed in accordance with the following principles:

Respect

Individuals have the right to privacy and confidentiality.

Transparency

People will be informed about how their information is used.

Consent

Consent will be obtained wherever required and appropriate.

Necessity

Only information that is relevant and necessary will be collected and shared.

Security

Information will be protected from loss, misuse, or unauthorised access.

---

4. Definition of Confidential Information

Confidential information may include:

Personal details.

Contact information.

Health-related information.

Wellbeing information.

Support records.

Risk assessments.

Safeguarding concerns.

Review documentation.

Volunteer matching information.

Complaints and feedback records.

Confidential information may exist in paper, electronic, verbal, or digital formats.

---

5. Definition of Consent

Consent means an individual's agreement for information to be collected, used, stored, or shared.

Valid consent should be:

Informed.

Freely given.

Specific.

Unambiguous.

Capable of being withdrawn.

Consent must never be assumed where it is required.

---

6. Obtaining Consent

Consent should normally be obtained:

During assessment.

Before sharing information with third parties.

Before using photographs or testimonials.

Before making referrals where appropriate.

Before participation in publicity materials.

Individuals should receive sufficient information to make informed decisions.

---

7. Explaining Consent

Before obtaining consent, individuals should be informed about:

What information will be used.

Why information is required.

Who may receive the information.

How information will be stored.

Their right to withdraw consent where applicable.

Information should be explained in a clear and accessible manner.

---

8. Recording Consent

Consent records should include:

Date obtained.

Information provided.

Purpose of consent.

Method of consent.

Any limitations or conditions.

Review arrangements.

Records should be stored securely.

---

9. Types of Consent

Consent may be obtained through:

Verbal Consent

Provided orally and recorded appropriately.

Written Consent

Recorded through forms or signed agreements.

Electronic Consent

Obtained through approved electronic methods.

The method used should reflect the circumstances and level of risk.

---

10. Consent for Service Delivery

Consent should normally be obtained before support begins.

This may include consent for:

Registration with the service.

Assessment activities.

Record keeping.

Routine communication.

Volunteer involvement.

Consent arrangements should be reviewed periodically.

---

11. Sharing Information with Volunteers

Only relevant information should be shared with volunteers.

Information shared should:

Support safe service delivery.

Help manage risks.

Respect confidentiality.

Volunteers should only receive information necessary to undertake their role safely and effectively.

---

12. Consent for Referrals

Before making referrals to other organisations, consent should normally be obtained.

The individual should understand:

Why the referral is being made.

What information will be shared.

Who will receive it.

Consent should be documented appropriately.

---

13. Consent for Photographs and Media

Written consent should normally be obtained before:

Taking photographs.

Using photographs.

Publishing stories or case studies.

Creating promotional materials.

Individuals should understand:

Where materials may appear.

How long they may be used.

Their right to withdraw consent where appropriate.

---

14. Consent for Feedback and Testimonials

Where personal comments, testimonials, or success stories are used:

Appropriate consent should be obtained.

Individuals should understand how information will be used.

Privacy should be respected.

Anonymous use should be considered where appropriate.

---

15. Confidentiality During Service Delivery

Employees and volunteers must:

Keep information secure.

Avoid unnecessary disclosure.

Discuss information only with authorised individuals.

Protect privacy during conversations and visits.

Confidentiality must be maintained at all times.

---

16. Sharing Information Within the Organisation

Information may be shared internally where necessary for:

Service delivery.

Safeguarding.

Risk management.

Supervision.

Quality assurance.

Access should be restricted to those with a legitimate need to know.

---

17. When Information May Be Shared Without Consent

Information may be shared without consent where:

There are safeguarding concerns.

Someone is at risk of serious harm.

There is a legal obligation.

A court order applies.

Criminal activity is suspected and disclosure is necessary.

Such decisions should be proportionate, justifiable, and documented.

---

18. Safeguarding and Confidentiality

Confidentiality does not prevent appropriate safeguarding action.

Where abuse, neglect, or exploitation is suspected:

Safeguarding procedures must be followed.

Relevant information may be shared.

The reasons for disclosure should be recorded.

Protection of individuals remains the priority.

---

19. Mental Capacity and Consent

Where there are concerns regarding an individual's ability to provide informed consent:

Capacity should be considered in accordance with organisational procedures.

Support should be provided to enable decision-making where possible.

Decisions should be documented appropriately.

Individuals should be assumed to have capacity unless there is reason to believe otherwise.

---

20. Withdrawal of Consent

Individuals may withdraw consent at any time where consent is the lawful basis for processing or sharing information.

Where consent is withdrawn:

Requests should be respected where possible.

Actions should be recorded.

Any limitations should be explained to the individual.

Withdrawal of consent should not disadvantage the individual unfairly.

---

21. Confidentiality During Home Visits

Employees and volunteers should:

Avoid discussing confidential information where it may be overheard.

Protect written records.

Store mobile devices securely.

Respect the privacy of service users and families.

Confidentiality arrangements apply both on and off organisational premises.

---

22. Email and Electronic Communication

When communicating electronically:

Approved systems should be used.

Recipients should be checked carefully.

Sensitive information should only be shared when appropriate.

Information security procedures should be followed.

Electronic communication should remain secure and professional.

---

23. Storage of Confidential Information

Information should be:

Stored securely.

Protected by passwords where appropriate.

Accessible only to authorised individuals.

Managed in accordance with retention requirements.

Security controls should reflect the sensitivity of information held.

---

24. Confidential Discussions

Confidential discussions should take place in appropriate settings.

Care should be taken to prevent:

Unauthorised access.

Accidental disclosure.

Conversations being overheard.

Privacy and dignity should always be respected.

---

25. Breaches of Confidentiality

Examples may include:

Sharing information without authority.

Sending information to incorrect recipients.

Discussing service users inappropriately.

Losing records or devices.

Unauthorised access to information.

All confidentiality breaches must be reported promptly.

---

26. Responding to a Confidentiality Breach

Step 1

Contain the incident where possible.

Step 2

Inform management immediately.

Step 3

Assess risks and impact.

Step 4

Follow data breach procedures.

Step 5

Document actions taken.

Step 6

Implement learning and improvements.

---

27. Records of Information Sharing

Records should be maintained of significant information-sharing decisions, including:

Information shared.

Purpose.

Recipient.

Date.

Consent status.

Rationale for the decision.

Good record keeping promotes accountability.

---

28. Training and Awareness

Employees and volunteers should receive training covering:

Confidentiality.

Data protection.

Information governance.

Consent procedures.

Safeguarding information sharing.

Training should be refreshed periodically.

---

29. Service User Confidentiality and Consent Flowchart

Information Required

↓

Explain Purpose of Collection

↓

Consent Required?

No

→ Proceed Under Relevant Lawful Basis

Yes

↓

Provide Information

↓

Obtain Consent

↓

Record Consent

↓

Store Information Securely

↓

Need to Share Information?

No → Continue Secure Management

Yes

↓

Consent Available?

Yes → Share Appropriately

No → Assess Legal/Safeguarding Basis

↓

Record Decision

---

30. Case Study

Scenario: Referral to a Community Support Service

A service user wishes to access a local wellbeing group but requires assistance with the referral process.

Action Taken

The purpose of the referral is explained.

The service user agrees to the sharing of relevant information.

Consent is recorded.

The referral is completed securely.

Outcome

The service user accesses additional community support and understands how their information has been used.

Learning Point

Obtaining and recording informed consent promotes transparency and trust.

---

31. Responsibilities

Board of Trustees

Responsible for:

Oversight of information governance arrangements.

Monitoring confidentiality and data protection compliance.

Directors

Responsible for:

Implementing this procedure.

Managing confidentiality and consent processes.

Responding to serious breaches.

Managers

Responsible for:

Supporting staff and volunteers.

Monitoring compliance.

Reviewing incidents and concerns.

Employees and Volunteers

Responsible for:

Maintaining confidentiality.

Obtaining and recording consent where required.

Reporting breaches or concerns promptly.

---

32. Monitoring and Quality Assurance

The organisation will monitor:

Consent records.

Information-sharing practices.

Confidentiality breaches.

Data protection incidents.

Training compliance.

Service user feedback.

Audit findings.

Monitoring findings will be used to improve information governance and service user confidence.

---

33. Review Arrangements

This procedure will be reviewed:

Annually.

Following significant confidentiality breaches.

Following safeguarding reviews.

Following legislative or regulatory changes.

Following audit recommendations.

Related Policies

Confidentiality Policy

Data Protection and GDPR Policy

Information Governance and Cyber Security Policy

Information Sharing and Confidentiality Procedure

Adult Safeguarding Policy

Mental Capacity and Decision-Making Policy

Records Management and Record Keeping Policy

Service User Rights and Responsibilities Policy

Associated Policies

Confidentiality Policy

Data Protection and GDPR Policy

Information Governance and Cyber Security Policy

Adult Safeguarding Policy

Records Management and Record Keeping Policy

Information Sharing and Confidentiality Procedure

Mental Capacity and Decision-Making Policy