AlchemHer CIC
Confidentiality Policy
Version 1.0 2025

1. Purpose

AlchemHer CIC is committed to maintaining the highest standards of confidentiality for all women accessing our services, including survivors of domestic abuse, coercive control, and toxic relationship trauma. This policy outlines how personal information is handled, protected, stored, and shared in accordance with UK GDPR 2018, the Data Protection Act 2018, the Domestic Abuse Act 2021, ICO guidance, safeguarding frameworks, and international digital privacy considerations.

2. Scope

This policy applies to all service users, staff, volunteers, directors, contractors, and partner organisations. It covers all personal, sensitive, and confidential information shared verbally, digitally, or in writing.

3. Principles of Confidentiality

All staff and volunteers will:

- Treat all information as confidential unless a safeguarding concern overrides this

- Only access personal data when required for their role

- Use the minimum information necessary

- Keep all private information stored securely

- Follow GDPR-compliant recordkeeping

- Maintain professional boundaries

- Respect survivors' rights to anonymity and privacy

4. What Information Is Considered Confidential

Confidential information includes:

- Personal details such as names, contact information, and addresses
- Trauma disclosures and experiences of abuse
- Mental health or wellbeing concerns
- Session notes and attendance records
- Digital identifiers such as usernames or IP addresses
- Photos, videos, audio, or any media shared
- Information relating to children or family members

5. Confidentiality in Virtual Services

Additional confidentiality protections apply:

- Participants are encouraged to join sessions from private, safe environments
- Headphones are recommended to prevent others hearing sensitive content
- Cameras are optional to protect anonymity
- Group content must not be shared outside sessions
- Recording, screenshots, or copying messages is prohibited
- Encrypted platforms and secure systems are used for service delivery

6. Limits to Confidentiality

Confidentiality may be broken without consent if:

- A participant is at serious risk of harm
- A child is at risk of harm
- Another adult is at risk
- There is evidence of trafficking, exploitation, or abuse
- There is involvement in serious crime, terrorism, or court orders
- There is immediate danger to life or safety

Individuals will be informed before information is shared unless this increases risk. For international users, UK safeguarding standards are applied as a baseline.

7. Consent and Information Sharing

Information may be shared with:

- The individual's explicit consent

- Statutory bodies when required by law

- Partner organisations only with written agreement and on a need-to-know basis

Participants may withdraw consent unless legally required otherwise.

8. Data Storage and Security

- Personal data is stored on encrypted, password-protected systems

- Access is restricted to authorised staff only

- Data is not stored on personal devices unless encrypted and approved

- Data is retained for 6 years unless regulations require longer

- Data disposal follows ICO guidance

9. Confidentiality for Staff and Volunteers

All staff and volunteers must:

- Sign a Confidentiality Agreement

- Receive confidentiality and boundaries training

- Report any breaches immediately

- Maintain separation between personal and professional communication

- Never share client information outside professional channels

Breaches may result in disciplinary action.

10. Confidentiality in Group and Community Spaces

To protect survivor safety:

- No recording or screenshots are allowed

- Personal identifiers should not be shared

- Unsafe or identifying content may be removed by facilitators

- Participants who breach confidentiality may be removed from the service

11. Handling Confidential Disclosures

Steps include:

1. Listen without judgment

2. Acknowledge the disclosure

3. Explain confidentiality boundaries

4. Record the disclosure if safeguarding applies

5. Follow safeguarding escalation procedures

6. Offer support or signposting

12. Breaches of Confidentiality

Breaches include:

- Sharing information without consent

- Accessing information unnecessarily

- Mishandling or losing data

- Discussing service users in informal or public settings

Breaches will be investigated under the Complaints or Disciplinary Procedure.

13. Training Requirements

All staff and volunteers receive:

- GDPR training
- Trauma-informed confidentiality training
- Safeguarding adults and children training
- Digital confidentiality and online safety guidance

14. Monitoring and Review

Confidentiality practices are monitored through:

- Annual audits
- Compliance checks
- Incident reviews
- Policy reviews after incidents or legislative changes

15. Approval

Signed:

Shyra-Marie Aaron Pryce

Director, AlchemHer CIC

Date: 17.11.2025