AlchemHer CIC – Data Protection & GDPR Policy

1. Introduction

AlchemHer CIC is committed to protecting the privacy, dignity, safety and personal data of all women who access our services. We recognise that survivors of domestic abuse, coercive control and toxic relationships may be at heightened risk if their information is mishandled or disclosed. We therefore operate to the highest possible data-protection standards, exceeding legal minimums wherever necessary to safeguard survivors.

2. Scope

This policy applies to all staff, directors, volunteers, moderators, contractors, partners, and service users. It covers the collection, processing, storage, sharing, and deletion of data across all services and digital platforms.

3. Legal & Regulatory Framework

We comply with: UK GDPR, Data Protection Act 2018, PECR, Domestic Abuse Act 2021, ICO survivor-protection guidance, UN Women digital safety standards, and WHO trauma-informed international data guidelines.

4. Data We Collect

Personal data may include: names or pseudonyms, email addresses, phone numbers, location/time zone, safeguarding concerns, emergency contacts, special category data (health, ethnicity, identity—always optional), technical data (IP, device info), and attendance logs.

5. How Data Is Used

We process data to: deliver services, ensure safety, respond to safeguarding concerns, improve programmes, comply with legal duties, maintain secure communications, and support equality monitoring. We do not profile users or use automated decision-making.

6. Lawful Bases for Processing

We rely on: Legitimate Interests, Vital Interests, Legal Obligation, and Consent (for marketing, recordings, and optional data collection). Consent is freely given, informed, and withdrawable.

7. Additional Protection for Domestic Abuse Survivors

Measures include: pseudonym use, secure communications, no voicemail without consent, no social media contact, restricted access to records, zero disclosure to third parties, rapid anonymisation, and enhanced risk-based confidentiality.

8. International Participants

Data is stored on secure UK/EU servers. We comply with international survivor-protection standards and only transfer data internationally when legally compliant (SCCs, adequacy decisions). No sensitive data is stored in countries with inadequate protection.

9. Data Storage & Security

Security includes encryption (AES-256), secure servers, MFA, strong password protocols, restricted access, encrypted backups, annual audits, training, and strict information-sharing protocols.

10. Data Retention

General participant data: deleted after 2 years of inactivity.

Safeguarding records: retained 6–7 years.

Financial records: 6 years.

Data can be deleted earlier upon request unless required for safeguarding or legal duties.

11. Data Sharing

Data may only be shared with: emergency services, safeguarding authorities, or approved partners—always minimal and lawful. We never share data with perpetrators, marketers, sponsors, or external agencies without consent or legal mandate.

12. Individual Rights

Users may: access, correct, delete, restrict, or object to data processing; withdraw consent; request portability; and avoid automated processing. Requests are completed within 30 days.

13. Data Breaches

Breaches must be reported internally within 2 hours. Serious risks are reported to the ICO within 72 hours. Affected individuals are notified promptly. Investigations and corrective actions follow immediately.

14. Staff Responsibilities

All representatives must: follow protocols, complete GDPR training, minimise data access, maintain confidentiality, use secure systems, and report breaches. Non-compliance may result in removal from the role.

15. Governance & Review

The Board reviews this policy annually or following incidents, legal changes, or organisational expansion.

16. Approval

Signed:

Shyra-Marie Aaron Pryce

Director, AlchemHer CIC

Date: 17.11.2025