Confidence. Skills. Employment Readiness.

wmn2wmn

Data Protection & Privacy Policy (UK GDPR Compliant)

Women 2 Women CIC | Company No: 17372913

Registered Address: 5 Brayford Square, London, England, E1 0SG

1. Policy Statement

Women 2 Women CIC is fully committed to compliance with the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. We respect the privacy of every individual and recognize that the fair, lawful, and transparent processing of personal data is critical to maintaining trust. This policy governs how we collect, store, handle, process, and safeguard all personal data concerning our participants (including young women and individuals aged 16–24 who are NEET), staff, volunteers, subcontractors, and organizational partners.

2. Data Protection Principles

All personal data processed by Women 2 Women CIC must be handled in strict accordance with the core principles mandated under Article 5 of the UK GDPR. Personal data must be:

- **Lawful, Fair, and Transparent:** Processed fairly, lawfully, and in a completely transparent manner in relation to the data subject.
- **Purpose Limitation:** Collected only for specified, explicit, and legitimate operational purposes and not further processed in an incompatible manner.
- **Data Minimization:** Adequate, relevant, and strictly limited to what is necessary for the purposes for which it is processed.
- **Accuracy:** Accurate and, where necessary, kept up to date; inaccurate personal data must be erased or rectified without delay.
- **Storage Limitation:** Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.
- **Integrity and Confidentiality:** Processed securely using appropriate technical or organizational measures to protect against unauthorized or unlawful processing, accidental loss, destruction, or damage.

3. The Types of Data We Process

To deliver our specialized employability, confidence-building, and mindset coaching programs, we process specific categories of data:

- **Personal Data:** Names, contact numbers, email addresses, postal addresses, dates of birth, emergency contact details, and records of employment or education history.
- **Special Category Data:** Due to our commitment to culturally sensitive, trauma-aware support and equality monitoring, we may process sensitive details such as racial or ethnic origin, religious beliefs, physical or mental health status, and details regarding disability status.
- **Lived Experiences & NEET Status:** Baseline socio-economic assessments to appropriately tailor our service delivery.

4. Lawful Bases for Processing

Women 2 Women CIC only processes personal information where a valid legal justification exists under UK law:

- **Consent:** Explicit permission granted by the participant (e.g., to join a program or receive promotional outreach). Consent can be withdrawn at any time.
- **Contractual Necessity:** Required to perform or fulfill an agreement with an individual, contractor, or service partner.
- **Legal Obligation:** Necessary to comply with a statutory law or legal requirement (such as safeguarding tracking or corporate accounting).
- **Legitimate Interests:** Required for the core operational execution of our non-profit mission, provided it does not override the fundamental privacy rights of the data subject.

5. Secure Data Management & Partner Hub Controls

Because our programs are delivered dynamically within external community hubs, local authority buildings, and partner spaces, strict operational data borders are enforced:

- **Digital Security:** All electronic data must be stored on highly secure, encrypted cloud platforms with multi-factor authentication (MFA) enabled. Data must never be saved locally on personal laptops.
- **Subcontractor & Freelance Mandate:** All freelance delivery staff and subcontractors are contractually bound by this data protection protocol. They are strictly prohibited from copying, downloading, or removing participant data from our authorized cloud ecosystem.
- **Physical Hub Vetting:** Paper documents containing personal details are strictly discouraged. If physical sign-in sheets or coaching logs are utilized within a partner hub, they must be securely locked away immediately and securely digitized within 24 hours.

6. Data Sharing & Third-Party Referrals

We respect participant confidentiality and only share individual information with external bodies (such as local authorities, housing associations, schools, or joint hub operators) under strict parameters:

- **Informed Referral Pathways:** Data sharing for program enrollment or employment progression tracking requires explicit, written consent from the participant.
- **Emergency Override:** Personal information may be disclosed without prior consent only if a critical safeguarding issue arises, or if a child, young person, or vulnerable adult is deemed at immediate risk of harm.
- **No Commercial Sharing:** Women 2 Women CIC will never sell, trade, rent, or distribute personal data to third parties for marketing purposes.

7. Individual Rights

Under the UK GDPR, data subjects possess robust legal rights regarding their personal data, which Women 2 Women CIC will actively uphold without undue delay:

- **Right of Access:** Request a complete copy of the personal information held about them (Subject Access Request).
- **Right to Rectification:** Request immediate correction of inaccurate or incomplete personal records.
- **Right to Erasure ('Right to be Forgotten'):** Request data deletion when it is no longer legally or operationally required.
- **Right to Restrict or Object:** Object to specific types of processing, such as direct communications or profiling.

8. Data Breach Notification Flow

In the highly unlikely event of a security failure leading to a data breach (unauthorized access, alteration, loss, or leak of personal information), the following statutory steps will be executed immediately:

- **Internal Reporting:** Staff or subcontractors must report the breach to the designated Safeguarding & Data Lead (Sommer Currie) within 1 hour of detection.
- **ICO Notification:** If the breach poses a material risk to the rights and freedoms of individuals, the Director will formally notify the Information Commissioner's Office (ICO) within 72 hours.
- **Subject Notification:** If the breach presents a high risk to individual privacy or safety, all affected data subjects will be notified directly and transparently without delay.

9. Governance & Review Framework

Director & Leadership: The Director retains final statutory accountability for ensuring organizational compliance with the UK GDPR and managing high-level legal risk.
Designated Data Contact: The Safeguarding Lead (Sommer Currie) acts as the practical point of contact for handling Subject Access Requests, security reviews, and internal team compliance.
Policy Review: This policy will be reviewed annually by leadership, updated whenever legislation changes, and published openly as an official asset on the company website.

Footnote: This is for informational purposes only. For medical advice or diagnosis, consult a professional. AI responses may include mistakes.