Womankind Bristol Women's Therapy Centre

Information Sharing & Confidentiality Policy

1. Introduction

1.1 Womankind is committed to maintaining the highest standards of confidentiality in all of our work in order to ensure the safety and wellbeing of our service users, volunteers, students and staff.

1.2 Womankind is also committed to safeguarding the rights of service users, volunteers and staff to access information which is held about them.

1.3 Womankind will work within the requirements of all relevant legislation including the following:

- The General Data Protection Regulation (UK GDPR) and Data Protection Act 2018
- The Human Rights Act 1998
- The Public Interest Disclosure Act 1998

1.4 Staff and volunteers should seek to establish the highest ethical standards in their work and have a duty of care to ensure that all interactions, verbal, written or electronic are carried out to comply with this policy. All staff, students and volunteers will be given an induction, which will include reference to this and other policies and procedures which they will be required to adhere to. Students and volunteers will also be required to sign a volunteer agreement which requires them to abide by Womankind's guidelines, policies and procedures, prior to starting their voluntary work or placement. Breaches of confidentiality may have serious consequences for service users and could therefore be the subject of staff disciplinary action or termination of volunteer/student placements.

2. Related policies and procedures

- Data Protection Policy
- Client Confidentiality and Data Protection Policy
- Staff Privacy Notice
- Job Applicant Privacy Notice
- Safeguarding Adults Policy
- Safeguarding Children Policy

3. Responsibility to service users

3.1 Informing service users

Any information relating to service users held by Womankind will be treated as confidential and will only be shared with other Womankind staff on a need to know

basis. This means that staff and volunteers will endeavour to create an environment where information about any service user will not be divulged or discussed casually. This includes but is not limited to access to service user's notes, records, case discussion and supervision.

However, there are legal exceptions to this rule, (see below section 3.4 'breaching confidentiality') therefore, service users should be informed about the circumstances in which Womankind would be required to share information with or without their consent, as per Womankind's Client Confidentiality and Data Protection Policy. This allows service users to give personal information to Womankind in an informed manner.

3.2 Contact with service users

Contact with clients, whether by telephone, electronic communication or in person, should be conducted in a confidential manner and secure environment, whether this is on Womankind premises, an outreach site, or whilst staff or volunteers are working from home.

Particular care should be taken to ensure that information is not disclosed inappropriately when returning client telephone calls and leaving messages. The Helpline Policy and Guidelines for Calls provides detailed advice for Helpline volunteers on receiving and making calls and leaving messages.

Staff and volunteers should maintain appropriate professional boundaries in their contact with clients and ensure that the confidentiality of other staff/volunteers/service users is maintained. The extent of the boundary will vary according to the nature of the role – e.g. on the Helpline/Webchat, callers do not need to disclose their identity, and the volunteers should not give out personal information and may even choose to use a pseudonym. In contrast, a volunteer Befriender who will visit a client weekly for a year, will be sharing more information about themselves, but within the context appropriate to supporting a vulnerable woman with mental health problems.

3.3 Sharing information with other agencies

No information held within Womankind about a service user will be given to any other person or agency without consent from the service user unless there are legal exceptions (see section 3.4 'breaching confidentiality'). This includes information about whether or not the service user uses (or has previously accessed) the service.

Partnerships, inter-agency working and referral relationships may require some information about service users to be shared. It is best practice to explain to a service user at the start of a service that, in certain circumstances, it is beneficial to share some information: e.g. to improve safety of service-users and their access to support. Consent should be sought and recorded (or a record made of express verbal consent where this is not practicable,) and should list the agencies with whom information will be shared. This would include the service user's GP who should be made aware of the counselling or group work being undertaken with the service user at Womankind and written consent from the service user to do so. Consent should also be obtained from the service user concerning notification of the GP in case of concern for their welfare, using Womankind's Medical Release Form . Any additional information which

emerges during the work with Womankind would require consent to be gained and evidence of consent must also be recorded.

Relationships with other agencies will be as co-operative as this policy allows. It must be made clear to other agencies from whom Womankind may receive information that Womankind operates an 'open file' policy meaning that the information they provide may be shared in the case of a subject access request. Similarly, Womankind staff must be aware that any information which they provide to other agencies may be given to the service users should they make a subject access request to agencies with which Womankind shares information. Where external agencies have ongoing relationships with service users, all parties concerned will agree boundaries of confidentiality.

3.4 Breaking confidentiality

Information on service users will be kept confidential, unless consent to share that information has been given. There are some specific circumstances where Womankind will breach confidentiality without consent if required which are as follows:

- In order to prevent or lessen a serious threat to a service user or another's safety.
- Where there is a child protection issue (see Child Safeguarding Policy/Procedure).
- Where there is an allegation or reasonable suspicion of a vulnerable adult safeguarding issue (see Safeguarding Adults Policy/Procedure).
- Where Womankind is required by law to do so

Confidentiality must only be breached following consultation with your line-manager/supervisor or Womankind CEO. In the absence of the CEO, a member of the Board of Trustees, unless it is an identified emergency and to delay would increase the likelihood of harm to another individual.

If it is possible, and would not put the service user or another individual at risk of harm, the service user must be informed that we will need to breach confidentiality and the reasons for the disclosure. If this is not possible, the service user should be informed as soon as feasible following the disclosure.

Accidental breaches of confidentiality should be reported immediately to your line manager or Womankind CEO. The data breach procedures in Womankind's Data Protection Policy should be followed and any service users affected should be contacted with an apology and a copy of the Complaints Procedure. The Information Commissioner may also need to be informed.

All breaches of confidential information should be reported to the CEO in order to update and review our risk management procedures.

4. Responsibility to staff and volunteers

4.1 Under no circumstances will personal information relating to staff members and volunteers be given to any individual or organisation without written consent or the permission of that person unless Womankind is required by law to do so, or in the case of one of the following circumstances:

- In order to prevent or lessen a serious threat to a service user or another's safety.

- Where there is a safeguarding concern (see Children and Adult's Safeguarding Policies and Procedures).

4.2 Post employment and volunteering

Confidential information obtained by staff and volunteers during the course of their employment or volunteering duties with Womankind cannot be shared by former staff and volunteers with a third party after the termination of employment or after they have finished volunteering. Legal remedies may be sought if such action comes to light.

5. Requests for information from third parties

5.1 Service performance and monitoring information

Monitoring information requested by third parties should never identify individuals or individual cases. Monitoring information may be given in the following formats:

- As statistics.
- Written case histories/studies, for publication or training purposes, should be composites or by changing some details such as the service user's name, age, circumstances and lifestyle. If a case history requires detail of a nature which could identify an individual, permission should be sought to use the story in an anonymous way.
- Case histories used for research should only be forwarded with the express permission of the subject, and in an anonymised way.
- No details of individual service users can be given to the media, or used on a website or other publication without the express consent of the individual. Full support should be offered to any service user who is willing to be interviewed directly by the media (i.e. press, radio, TV etc).

5.2 Police requests for therapy notes

Womankind's Pre-trial Therapy Policy provides clear guidance on working with survivors of sexual violence who have chosen to report to the police and have an ongoing criminal investigation or court case pending. This policy should be read and adhered to at all times.

Any police requests for client records or therapy notes should be directed to the Clinical Manager. Written consent from the service user will always be sought before disclosing therapy records or notes.

6. Sharing information securely

It is important we take appropriate steps to protect individual's confidentiality when sharing any personal information with other parties.

Where possible we will use the CJSM secure email system to share confidential service user information with third parties. When this is not feasible, confidential

electronic information will be password protected before sending it by email (and the password notified separately, e.g. by text).

Any confidential information received by email from external agencies or individuals will be saved securely and deleted from emails.

7. Record keeping and storage of confidential records

7.1 Note recording and personnel /supervision recording

Service user, staff and volunteer records are the property of Womankind and will be stored in accordance with this policy (see point 7.2). Records will not be removed by any member of staff, whether paid or voluntary, without prior consent from the Womankind CEO or Chair.

Womankind follows the principles and guidelines set out in the NHSX Records Management Code of Practice 2021, and utilises this document for reference.

The General Data Protection Regulation (UK GDPR), which came into force in May 2018 requires us to only use your information in ways that are lawful. This is further explained in Womankind's Data Protection Policy.

The Data Protection Act 1998 states that records must be adequate, relevant and not excessive.

- Notes should summarise the main points of discussion. They should distinguish between fact and opinion, avoid emotive words, and avoid use of jargon or abbreviations.
- Notes should be completed as soon as reasonably practical after a meeting, and rough contemporaneous notes should be destroyed after a formal record is made.
- Contemporaneous notes made during a meeting should be destroyed by shredding as soon as the notes are written up.
- Notes should clearly indicate author, recipient and date, and have a clear list of actions.
- Notes should be stored either electronically, e.g. on the secure case management system and protected by backup, or on paper in a secure filing cabinet, but should not normally be duplicated across both systems.

7.2 Storage of information; Any recorded information on service users, ex-service users, staff and volunteers will be:

- Kept in secure storage.
- Protected by the use of passwords if kept on a computer.
- Recorded by codes if used for statistical purposes so those individuals remain anonymous.

- Retained for no longer than is necessary, as per the data retention periods stated in our Data Protection Policy.

8. Access To Information

8.1 Service user files – Staff and volunteers are required to keep notes and records which are maintained in accordance with GDPR and Data Protection Act requirements. Our Client Confidentiality and Data Protection policy should be displayed in the main offices/reception area and a copy shared with new clients when starting counselling or in the befriending service.

Service users have a right to access their own files and should be informed of this right. Responses to Subject Access Request must be undertaken within 40 days unless it is unreasonable to do so within this time, in which case the service user must be informed of the timescale within which they will be given the information.

Under a Subject Access Request the service user has the right to see third party reports, even if the author does not authorise them for release. However, the report may need to be redacted to prevent identifying without consent the author of the report or any other individual. If the content of the report is anonymous but would still allow a third party to be identified then this information may be withheld unless you have that person's consent to release the information.

In most cases the information must be provided as a copy in a permanent form, i.e. a photocopy of the documents which have been deemed appropriate to provide. However, those who have requested the information electronically may be satisfied or prefer an electronic copy, so it is helpful to clarify the person's preference.

Womankind's service users have the right to know if personal data is being held about them and will be given:

- A description of personal details held about them.
- The purposes for which Womankind uses this personal data.
- Those to whom Womankind may disclose this personal data.

Workers will ensure that service users have access to personal information held by the agency on request. Care however needs to be given not to disclose information gained from other sources, which may identify the personal data of a third party, unless they have consent to do so. Access to personal information must be granted unless there are good reasons for refusing access. These include:

- The information may cause harm to the service users' (or another person's) mental or physical condition unless an appropriate health professional has been consulted.
- The identity of person making the request has not been confirmed.
- Womankind recently complied with a similar request.

Individual service users are entitled to correct any personal information by

- Requesting a correction

- Requesting that a correction statement be attached to the information

8.2 Staff and volunteer files/records –Staff and volunteers have the right to access their own files and personal records and should be informed of this right. Access to files and personal records will be arranged at the earliest opportunity by the Womankind CEO, a senior member of staff or a member of the Board of Trustees.

Written material received from outside agencies may be disclosed to the staff member or volunteer to whom it relates, unless clearly marked 'confidential' by the author. This policy must be made clear to outside agencies from whom written material is sought.

9. Disposal of records

Any confidential records will be permanently deleted and/or safely destroyed by shredding in accordance with Womankind's Data Protection Policy.

Policy approved by: Womankind Board of Trustees

Date of approval: 18th July 2022

Date of next review: July 2025