Confidentiality Policy

1. General Principles

1.1. It is recognised that the use of information about individuals and organisations during the course of their work and activities will be used. In most cases it will not be stated as confidential and it will be necessary to use common sense and discretion in deciding whether information is expected to be confidential.

1.2. Exchanging personal information about individuals with whom they have a personal relationship with should be avoided.

1.3. It is not appropriate to discuss a personal sexuality without their prior consent.

1.4. Talking about organisations or individuals in social settings should be avoided.

1.5. Information considered sensitive, personal, financial or private should no be disclosed to anyone without their knowledge or consent.

1.6. If it is deemed necessary to discuss difficult situations with someone else to gain a wider perspective on how to approach the problem, consent must be sought before the personal information enters any discussions unless it is beyond doubt that the organisation would bot object this. Alternatively, a discussion may take place withholding personal identifying information, thus remaining confidential.

1.7. Where there is a legal duty to disclose information, the person wo whom the confidentiality is owed will be informed that disclosure has or will be made.

2. Why information is held

2.1. Most information held related to organisations which supports o funds them o the individual who attend their sessions.

2.2. Information is kept to enable to keep in touch with customers in the form of a of newsletters or email.

2.3. As an organisation we have the role in putting people in tough with community organisations, suppliers and keeps contact with details which are passed on to any enquirer, except where the group or organisation expressly requests that the details remain confidential.

2.4. Information about ethnicity and disability of users is kept for the purposes of monitoring equal opportunities policy.

3. Access to information

3.1. Information is confidential to the organisation and may be passes to others within the organisation to ensure the best quality service for users.

3.2. Where information is sensitive, where it my contain information regarding legal issues or disputes, it must be labelled confidential and should state the names of those involved.

3.3. Users may have access to their records held by the organisation by giving 14 day notice in writing and be signed by the individual.

3.4. When photocopying or working on confidential documents, they must ensure they are not accidentally seen by others. This also applies to information on computer screens.

4. Storing information

4.1. General non confidential information bout organisations is kept in unlocked filing cabinets.

4.2. Personal information will be kept in a lockable filing cabinet.

4.3. Files or filing cabinets with confidential information should be labelled confidential.

5. Duty to disclose information

5.1. There is a legal duty to disclose some information including:

5.1.1. Child abuse will be reported to Social Services and police.

5.1.2. Drug trafficking, money laundering, acts of terrorism or treason will be disclosed to the police.

5.2. In addition, if it is believed that an illegal act has taken place, or that a user is at risk of harming themselves or others, they must report this to the appropriate authorities.

5.3. Users should be informed of such disclosures.

6. Disclosures

6.1. Disclosure of information is always kept separately from personal file in secure storage with access limited to those entitled to see it as part of their duties. It is a criminal offence to pass this information to anyone who is not entitled to receive it.

6.2. Documents will be kept for a year and then destroyed by secure means. Photocopies will not be kept, however it may be necessary to keep a record to the date of issue of a disclosure, the name of the subject, type of disclosure requested, position or which disclosure was requested, unique reference number of the disclosure and the details of the recruitment decision taken.

7. Data Protection Act

7.1. Information about individual, whether on the computer or on paper, falls within the scope of the Data Protection Act and must comply with the data protection principle. These are that personal data must be:

- Obtained and processed fairly and lawfully. Held only for specified purposes.

- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept longer than necessary
- Processed in accordance with the Act
- Kept secure and protected
- Not transferred out of Europe.