CONFIDENTIALITY POLICY & PROCEDURE

1. General Statement of Policy

1.1 This policy is intended to protect service users, staff and volunteers from the possibility of information about them being passed on to individuals or organizations who have no right to that information. Reference should also be made to the policies relating to Complaints and Grievance and Volunteering and to the Data Protection Act.

1.2 South Lakeland Mind understands confidentiality to mean that no information regarding a service user of SLM shall be given directly or indirectly to any third party which is external to the staff, volunteers, Chair of Trustees and Board of Trustees, without the service users prior expressed consent to disclose such information except where there is a question of serious risk to a person(s), or there is a statutory obligation to do so. (See items 2 and 3 below).

1.3 SLM recognises that information may be shared through staff, volunteers or trustees discussing individual service users in order to provide the best possible service to particular individuals.

1.4 Confidentiality is an essential component of an accessible service. By providing an assurance of confidentiality SLM can enable a user to disclose a problem that they previously may not have been happy to discuss with anyone else. People contacting SLM need reassurance that they will not be judged and that any information they give will not be shared with others without their knowing and giving their authority. (See items 2 and 3 below for exception to the confidentiality rule).

1.5 Unauthorised breach of confidentiality will be considered as a serious case of misconduct and could lead to disciplinary action.

2. Protecting Confidentiality

2.1 Awareness: All staff and volunteers, as part of their induction, will be made aware of South Lakeland Mind's Confidentiality policy and how it affects them in their role.

2.2 Everyone working or volunteering for South Lakeland Mind is expected to have an understanding of the confidentiality policy and its importance. This includes trustees, staff and volunteers.

2.3 All staff, trustees and volunteers will be asked to sign a statement confirming they will maintain confidentiality as stated in this policy.

2.4 Photographs of events and activities can be useful in recording and illustrating our services but staff and volunteers must not take a photograph of a service user or pass it to an outside body or person, publish it or include it in a document without the express permission of the individual concerned. Service users may take their own photographs for personal use but only with the consent of the subject(s).

3. The Freedom of Information Act

This contains particular statutory requirements to release information in the following circumstances:

- Reporting of notifiable diseases to the Director of Public Health where appropriate.
- Reporting accidents at work, in certain circumstances, to the Health and Safety Executive.
- Replying to certain specific enquiries from government departments e.g., Dept. of Employment, Dept. of Social Security or Inland Revenue. Not all such enquiries are covered by statutory requirements so a check on the legal status of the request should be made before supplying information.
- Under the Prevention of Terrorism Act 2005, a legal obligation to break confidentiality and pass on information on terrorist activities.
- Money laundering.
- Offences under the Misuse of Drugs Act
- Giving evidence in court if a subpoena is issued.

This list is by no means exhaustive and any doubt about disclosure should be referred to the Chief Officer.

4. Duty of Care

4.1 SLM owes a "duty of care" to the users of its services. It may therefore be necessary to breach confidentiality where a service user is acting, or likely to act, in a way that could cause serious harm to him / herself, or put others at risk.

4.2 SLM also owes a more general duty of care towards members of the public. It may be necessary to pass on information to the police or statutory authorities where there is considered to be a serious risk to a particular person or persons, or to the public in general.

5. Disclosure of Crime

5.1 There may be instances where service users confide that they have committed/are about to commit a crime. In English law there is no duty to disclose a criminal offence so being aware of the crime is not assisting in that crime.

5.2 The exception to this is under the Prevention of Terrorism legislation which makes it an offence to fail to give information which may help to prevent acts of terrorism or apprehend a terrorist.

5.3 It is however, an offence to aid, abet, counsel or procure the commission of an offence. It is therefore important that the staff member/volunteer makes sure s/he does not give, or in any way can be seen to be giving, encouragement or assistance.

5.4 If a staff member or volunteer has concerns about the information the user is disclosing, he/she must tell them that:

- What they are saying/about to say could break the law.
- They can be assured of confidentiality but need to be warned not to give any further details. They should seek advice from a solicitor.
- They may be later summonsed as a witness.

5. Procedures

6.1 SLM recognises that occasions may arise where individual staff or volunteer workers may feel they need to breach confidentiality. The charity recognises, however, that any breach of confidentiality may damage the reputation of the charity's services and therefore has to be treated with the utmost care.

6.2 On occasions where a staff member or volunteer feels confidentiality should be breached the following steps must be taken:

- The staff member or volunteer should raise the matter immediately with the Chief Officer or in his absence the Chair of Trustees.

- The issues involved in the case should be outlined and an explanation given why it is felt confidentiality should be breached and what would be achieved. A written record should be made of the discussion.

- The Chief Officer is responsible for discussing with the staff member or volunteer what options are available in each set of circumstances.

- The Chief Officer is responsible for making a decision on whether confidentiality should be breached. If the Chief Officer decides that confidentiality is to be breached then he should take the following steps:

    a. In the first instance the Chief Officer should contact the Chair or Vice Chair of the Executive Committee and brief them on the full facts of the case, ensuring they do not breach confidentiality in doing so.
    b. The Chief Officer should seek authorization to breach confidentiality from the Chair/Vice Chair.

6.3 If the Chair/Vice Chair agrees to breaching confidentiality, a full written report on the case should be made and any action agreed undertaken. The Chief Officer is responsible for ensuring all activities are acted upon. If the Chair/Vice Chair does not agree to breach confidentiality then this is the final decision of the organization.

7. Access to information and records

7.1 Reference should also be made to the Data Protection Policy.

7.2 Only information, which is accurate, relevant and appropriate, should be kept on file. Service users have the right to see information held about them. They can access it as long as they give notice of their intention to do so. However access to files, letters, reports and case notes written by third parties (eg SW or CPN) should be at the discretion of the Chief Officer, who may need to seek permission of the third party beforehand. The file documents cannot be removed from the SLM office but photocopies may be taken. Service users and volunteers should be told what information will be kept on file and who will have access to it.

7.3 The maintenance of adequate safeguards in record keeping and the adherence to the confidentiality procedures is essential. Confidential records, files or any other information relating to service users must be stored in a secure place and access to them controlled. Records containing personal data should be kept in locked filing cabinets or drawers and the keys kept securely.

8. Disposal of Records

All records containing personal and/or sensitive information should be destroyed once there is no longer any need to keep the information. It is the responsibility of the Chief Officer to ensure that disposal of confidential information is dealt with in accordance with the Data Protection Act (see Data Protection Policy).

9. Complaints

Where a complaint of breach of confidentiality is received it will be dealt with in accordance with SLM policy and procedures on Complaints and Grievance.

10. Ensuring the Effectiveness of the Policy

All Management Committee members will receive a copy of the confidential policy. Existing and new workers will be introduced to the confidentiality policy via induction and training. The policy will be reviewed annually and amendments will be agreed by the Management Committee.

This policy is intended as a statement of intent and does not constitute a binding contractual or personal agreement. But it will be monitored and revised in the light of service user, staff or volunteer experience or comments and any operational changes and legislative or other external considerations. Interpretation and any matters not specifically covered by the policy will be decided by the Chief Officer and / or Trustees.

Policy Approved by Board of Trustees: April 2010

Revision(s) approved: 14th August 2014

Review Date: March 2015

If at any time it seems appropriate to review the policy sooner than the review date, such as through a change in the law, then this should be done without delay.