Moor Allerton Elderly Care

CONFIDENTIALITY POLICY

This policy sets out

1. **Principles**

a. We are committed to providing confidential services to users. We believe the principle of confidentiality must be integrated across all aspects of our services and management.
b. Information is confidential to MAECare as an organisation and may be passed to colleagues, line managers or trustees to ensure the best quality service for users.
c. Service users, paid staff, trustees and volunteers have the right to expect that any information they impart and held by us will:

- only be used for the purpose for which it was given
- not be divulged to any other third parties without consent unless MAECare is permitted or required to do so under the law.

d. The policy applies to all staff, volunteers and members of the Board of Trustees and is intended to protect the rights of clients and service users, members of staff, trustees, volunteers and the interests of the organisation.

e. This policy also covers the confidentiality of information on the internal workings and business affairs of the organisation e.g. supplier and accounts information

f. This policy covers all information held by us in whatever form, e.g. on paper, on the Charity's IT systems, laptops, emails and external electronic storage devices, including memory sticks and external drives (see ICT acceptable usage for further information.

2. **Consent to Record Information**

MAECare obtains consent:

- Verbally: when people sign up to activities we ask them if we can put their details on the database so they can receive the newsletter
- Written: when a formal assessment is done the staff member confirms that they are willing for their information to be on the database.
- Membership form or letters with the newsletter imply that information is being kept but do not ask for explicit consent.
- Emergency contacts form implies consent to share information within MAECare

3. **Consent to information sharing.**
    - MAECare does not share information about service users with other agencies unless we have received their permission. We do not make

referrals to other agencies without permission. We do not share service users' information with concerned parties such as neighbours.

- MAECare does not share addresses or telephone numbers of service users with other service users without their permission.

4. **Breaching confidentiality**
   Confidentiality will only be breached in exceptional circumstances and only after discussion with the Project Manager. Situations where confidentiality may have to be breached may include:-

- A person is in a life threatening situation
- A situation where inaction might place them/someone else in a life-threatening situation.
- A person is being maltreated, abused or exploited.
- Where inaction could lead to someone within the project being harmed.
- Legal issues such as someone a criminal investigation

The decision to break confidentiality should NEVER be taken by a staff member or volunteer alone unless in an emergency. Each circumstance will be discussed with the project manager. In the event that the Project Manager is unavailable then her deputy or a named management committee member will make the decision

5. **Confidentiality procedures**

- Verbal information: great care is taken in discussing service user situations. This is not done in the public area of the office.
- Information is shared with volunteers in situations where this supports working with that service user (e.g sharing the fact someone has memory loss). Volunteers need to know to ensure the person is safe to use the right strategies to engage with them.
- Individual circumstances are not discussed at the management committee meetings, members are asked to discuss their concerns with the project manager
- Written information including case studies and reports to management committees will always be anonymised so that the service user can not be identified
- Securing information – MAECare keeps written information to a minimum. Case notes should not be stored in staff cars and should not be taken home unless absolutely necessary (for example if a visit is at the end of a working day or at the weekend)
- Care should be taken when using computer screens that members of the public cannot see the information
- Registers and other lists with details of service users' addresses and telephone numbers are kept in folders by the tutor or leader of the group.
- Staff information is password protected.
- Information held on the database is password protected as is secured along with the rest of the data in the organisation
- Monitoring information which is sent to funders is always anonymised.

6. **Storage of DBS checks information**.

- All DBS checks are carried out electronically and a unique number is received. If the DBS check is clear the number is recorded on the database record for volunteers and a personal details file for staff.
- DBS information is not stored with staff personnel files.
- ID information is only stored until the DBS unique number is received. ID information will then be shredded.

7. Data Protection Act.

Information held about individuals, whether on computer or on paper, falls within the scope of the Data Protection Act and must comply with the data protection principles. 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.

Approved November 4th 2014

Signed

Muriel Ramsey