

OPTIONS FOR LIFE

DATA PROTECTION POLICY

The Data Protection Act 1998 extends the rights given to individuals in previous legislation, and requires 'data controllers' (people or organisations that hold and process details of living individuals) to comply with the eight principles (rules governing the use of personal data) and bear in mind the rights and freedom of those individuals when processing their details.

Options for Life is the 'data controller' under the Act, and is therefore ultimately responsible for implementation. However, there is a specific exemption from notification for a data controller which is a body or association not established or conducted for profit, and assuming the organisation meets other criteria. Options for Life meets this criteria.

Options for Life will hold the minimum personal information necessary to enable it to perform its functions. All such information is confidential, and needs to be treated with care, to comply with the law.

All staff and volunteers will be made aware of this policy and the related procedures, and will be adequately trained.

Any breach of the Data Protection policy and the associated procedures, whether deliberate or through negligence, will result in disciplinary action in the case of members of staff. Appropriate action will also be taken in the case of any volunteers, service users or other persons who do not comply with the Data Protection policy and the associated procedures. Any breach of the Data Protection policy and the associated procedures may result in a criminal prosecution.

This policy was approved and endorsed by the Board of Trustees on 16th November 2009, with next review due on 16th November 2010.

Data users must comply with the Data Protection principles of good practice which underpin the Act.

These state that personal data shall:

1. be obtained and processed fairly and lawfully (that the subject of the data has consented to its collection and use)
2. be held only for specified and lawful purposes, and not be processed in any manner incompatible with those purposes
3. be adequate and relevant, but not excessive
4. be accurate and kept up to date
5. be kept for no longer than necessary
6. be accessible to data subjects
7. be subject to the appropriate security measures to protect against unauthorised or unlawful processing and accidental loss, destruction or damage
8. not transferred outside the EEA (European Economic Area)