Appendix 6 - CONFIDENTIALITY POLICY

A6.1 Confidentiality is the protection of information given by or about any client seeking the assistance of H & F MIND. Confidentiality is between the client and the organisation and not between the client and the individual worker. Where external supervision is used, the supervisor concerned is deemed to be an employee of the organisation and the policy of confidentiality applies in that information may not be taken outside of this setting without the explicit permission of the client concerned.

A6.2 All information concerning a client should only be discussed in a professional capacity where such discussion is deemed necessary in the service of the client's needs. Clients and their circumstances should not be discussed with families, friends, and other clients, other workers not concerned with the case or in any public setting without the client's permission.

A6.3 Information obtained for one purpose may not be used for another without the client's explicit consent except as qualified below.

A6.4 Staff are responsible for ensuring that clients and referring agencies are aware of the organisation's policy concerning confidentiality, and for ensuring that it is explained to them in terms they can understand. It should be made clear that information is given to a worker as a representation of the organisation and it may need to be shared selectively with other members of the organisation in order effectively to assist the client.

A6.5 The right to confidentiality may be overridden where there is evidence that failure to disclose information might:

a) endanger the client's own life or that of another; and/or

b) seriously endanger the community; and/or

c) cause a serious threat to the worker

A6.6 The disclosure of personal information to the police may exceptionally be justified if it can help to prevent, detect or prosecute a serious crime (see next paragraph). Before such disclosure is made the following conditions at least must be satisfied:

- the crime must be sufficiently serious for the public interest to prevail. Section 116 of the police and Criminal Evidence Act 1984 provides a guide to what constitutes 'serious crime' but it should not be treated as either conclusive or exhaustive.

- it must be established that, without the disclosure, the task of preventing or detecting the crime would be seriously prejudiced or delayed.

- satisfactory undertakings must be obtained that the personal information obtained will not be used for any other purpose and will be destroyed of if the person is not prosecuted, or is discharged and acquitted, the request must be from a police officer of suitably senior rank, e.g., superintendent or above

- all decisions regarding disclosure to the police must be approved by the Director and the Management Committee informed.

A6.7 All decisions to breach confidence must remain strictly limited to the needs of a given situation at that time, must be discussed with the line manager and recorded in the case file.

A6.8 Where it is judged to be necessary to share confidential information with another agency. the client should be contacted before doing so, and their permission sought, unless it is clearly recorded that their permission has already been given. Exceptionally, some information may be shared with an outside agency without prior consultation (such as a N.A.I. case conference). The client should be informed in such a case that confidential material has had to be shared, and why.

A6.9 Computer systems should be secured against unauthorised access or amendment and against loss through accidental or deliberate damage, erasure or disclosure. Failure to take reasonable care could result in an action for compensation under section 23 of the Data Protection Act 1984. Only authorised members of staff should be allowed direct access to the case record systems. Pseudonyms, case numbers etc. should be employed. Screens of video display units should be located so that they are not open to view by unauthorised people.

A6.10 Manual records, including indexes and computer printouts, should be secured against unauthorised access or amendment and against loss through accidental or deliberate damage, erasure or disclosure. They should be located insecure metal cabinets. Records should not be taken out of the building, but where this is necessary, extreme care should be used in ensuring that no material is lost or damaged in the process. Any manual records that it is no longer necessary to retain must be shredded prior to disposal. Under no circumstances must any manual records be discarded in any other manner.

A6.11 No question involving confidential information should ever be answered over the telephone without establishing the identity and authenticity if the caller - and if necessary confirming with a manager if it is appropriate to impart the information. Any press queries should be referred to the Director.

A6.12 All members of staff should be routinely be asked to read the policy on confidentiality and should be made aware that the disciplinary procedures will apply for

breaches of the policy. Managers at all levels have a responsibility to ensure that their staff preserve confidentiality.