APPROVED

Policy on Confidentiality in respect of Service Users and their Families

The Main Principles

1. Confidentiality refers to the limited use of information about service users and their families that is obtained by staff during the course of their work. In certain circumstances there may be limits to confidentiality, for example, when safety or legal issues arise.

2. The Policy on Confidentiality is informed by Personal Outcome Measures which require:
   a. that people decide when to share personal information and to whom and in what circumstances the information should be shared,
   b. that the organisation has systems and processes in place to maintain the confidentiality of information,
   c. that the service users and parents of children give permission for information to be shared,
   d. that service users and parents of children are fully informed about what information is released, to whom and for what purpose, and
   e. that service users and parents of children have easy access to the information that is held.

3. Written consent must be sought from service users or parents of children as to who has access to their personal information. Each file should have a list of the key professionals who, with the agreement of the service user or parents, may access personal information. This consent should be reviewed at regular intervals and the signed consent placed on the service user's file. Service users should be supported by staff and through training in order to ensure that they are giving informed consent.

4. Service users and parents of children have the right to access the information that is held and where necessary service users should be appropriately supported to read or hear the content of files.

5. No personal information relating to service users should be visible in programme areas or in people's homes, for example, behaviour schedules or diet sheets should be stored in a manner that is accessible to those who need to see them but not visible to anybody else in the area.

Signed: _____
Patrick McGinley, Director of Services

Date: 19 September, 2005

Policy No: 1997/01 - Version 2
Implemented on 21st April 1997

Implementation Date: 1st October, 2005

6. The onus is on Managers or Head of Departments to create a climate of confidentiality in their service community. In addition, all individuals working, training, and volunteering within the service are required to make themselves fully aware of the confidentiality policy.

7. As part of this climate of confidentiality staff should be aware of where and when they speak about service users.

8. It is anticipated that staff and others, including service users, as appropriate will need to be informed of pertinent issues regarding service users in order to provide the best possible service. All such individuals must be reminded by senior colleagues to maintain the confidentiality of information received.

9. When service users and their families commence receiving a service from the Brothers of Charity Services the Agency's Policy on Confidentiality must be explained to them and a copy of the Policy should be made available to them.

10. Privileged information must be kept in accordance with the files policy. Reference to the existence of privileged information and its location must be attached to a service user's file.

11. Reports should be specific and clear as to the purpose for which they are being written.

12. In general, permission of the author of a report should be obtained before it is photocopied. In the case of requests under the Freedom of Information Act, copies of files are forwarded to requesters without seeking permission from authors.

13. In general, personal details about service users should not be discussed when people not directly involved with the service user are present. However, there are occasions where people less directly involved must be provided with information to ensure the best possible service.

14. Information about one service user should not appear in another service user's file. However, there are some circumstances where it is appropriate for the name of service users or their initials to be documented. For instance, in the case of friendships or where there are safety concerns.

15. Information contained on data bases or in e-mails should be treated with the same concern for confidentiality as any other information held on service users.

The Policy Statement

Definition
Confidentiality refers to the limited use of information about service users and their families that is obtained by staff during the course of their work. This information should be treated with the utmost respect at all times in order to preserve the service user's right to privacy and to establish and maintain a good working relationship. These principles should be borne in mind at all times when gathering and sharing information.

Climate of Confidentiality
The duty of confidentiality extends to all staff. The onus is on Managers/Heads of Departments to create a climate of confidentiality in their service community. It is their responsibility to

ensure that all staff, including temporary staff are made aware of the Agency's Policy on Confidentiality. It is the responsibility of any person who supervises students within the Agency to ensure that the student has been made aware of the Agency's Policy on Confidentiality and makes every effort to ensure that the student adheres to it.

Sharing of Information and Limits to Confidentiality
It will be necessary to share information about service users with others on the team providing the service. On occasion, it may be necessary to share information outside of the people directly involved with the service user in order to obtain advice and consultation. It should be noted that names should not be used during such consultations. In certain circumstances, the service user/parent of the service user may request that a piece of information is not shared. This request should be complied with except in circumstances such as suspected abuse or where it would be detrimental to the service user.

> *"Information clearly entrusted for one purpose should not be used for another purpose without explicit consent. Such information should only be divulged with the informed consent of the service user (or informant) except where there is clear evidence of serious danger to the service user, worker, other persons or the community. Any service user information to be shared must be directly relevant to and limited to the particular situation about which the information is required" (IASW'S Code of Ethics).*

The right to confidentiality by the informant may be over-ridden in circumstances such as suspected abuse or where there is evidence of serious danger to the service user, worker, other persons or the community. The withholding of information between professionals and between Agencies is not acceptable where failure to disclose may have an influence on the future safety and welfare of the service user. In situations of suspected abuse the Brothers of Charity Policy on Abuse must be followed.

Informing Service Users
When service users and their families are initially accepted into the Brothers of Charity Services, the Agency's Policy on Confidentiality must be explained to them and they should be offered a copy of the policy. They should be informed of the type of information which will be kept on file and on computer and who has access to this. They should be informed that in cases where the Agency is promoting new services or making a case for existing services certain limited information such as name and date of birth may be forwarded to the Department of Education or the Department of Health. They should also be informed that circumstances such as those involving safety may pose limits to confidentiality.

Commitment to Confidentiality
All staff already in the Agency, all new staff, and all those involved in our services, be they volunteers or students must be made familiar with this Policy on Confidentiality. In addition, they must sign a statement indicating that they agree to abide by its principles. This statement, located in Appendix 1, should be countersigned by their line manager.

Maintenance of Files
Files are maintained and kept in a secure manner as outlined in the Agency's File Policy.

Privileged Information
There will be occasions when certain information is recorded in a file to which access is restricted such as a designated file. This pertains to privileged information which typically relates to situations involving abuse, or sensitive information relating to the person's family. A reference to the existence of privileged information must be attached to the file so that it can be accessed if needed to ensure the best possible service provision.

Access
Access to files should be restricted to those staff directly involved with the service user. Volunteers and students on summer job schemes should not have access to files. Locum staff and students on placement with the Brothers of Charity Services as part of a recognised course should be allowed access to files at the discretion of their supervisor. It is the responsibility of supervisors to ensure that the person has read this Policy on Confidentiality and has signed a form agreeing to abide by it**.** Students may not have access to Files unless specific permission for access has been obtained from the service user/family/parents as appropriate. Students may have access to consult but not to photocopy files.

Old files
Information on service users who have left the service will be dealt with in accordance with the Brothers of Charity Services File Policy.

Reports
All reports must state the purpose for which they are written and should note to whom they are circulated. They should contain factual information or descriptions of direct observations. It should be clear when professional opinions or judgments are expressed and on what basis they are formed.

Reports to other Agencies
It is recommended that service users/families should be informed of what information is being sent to another agency in relation to the transfer of a service user. It is also recommended that consent be obtained from service users/families when forwarding information to other agencies.

Copying of Reports
In general, permission of the author of a report should be obtained before it is photocopied. If this person is unobtainable, permission should be sought from the relevant Head of Department or Head of Centre. However, in the case of requests under the Freedom of Information Act, files are forwarded to requesters without seeking author permission. If copies of reports are circulated at a meeting they should be returned to the Chairperson at the end of the meeting for shredding.

Faxing Reports
It is the Brothers of Charity Services policy not to fax reports or other confidential information relating to service users.

This policy may be set aside in exceptional circumstances, only when

- the author has given prior permission for the information to be faxed, and,

- there has been prior agreement that the person to whom the report is being faxed will personally receive the fax as it arrives at the destination.

Meetings
If the sharing of information at meetings appears to be in danger of breaching confidentiality, it is the responsibility of the Chairperson to draw attention to this and re-focus the discussion. The Chairperson should remind people at the start of meetings about the confidential nature of the matters being discussed. A number of service users and their families are members of centre and service teams. There is a need to make service users/families aware of confidentiality requirements and service users should be gradually introduced onto such teams while being provided with on-going training.

Copying of Case Conference Notes/Admissions Meetings
Copies of case conference notes circulated should be kept to the minimum number necessary. There are occasions, such as admission meetings, where a number of individuals are reviewed. Information pertaining to an individual service user and the outcome of the meeting may be noted on that service user's file. Information relating to other service users discussed at the meeting must not be documented in the files of other service users except in exceptional circumstances.

Verbal Information
To create a climate of confidentiality staff must be aware of where and when they speak about service users. Personal information about service users should not be discussed in coffee rooms, corridors, or public places. Visitors, including families when visiting a Centre, should only be given information about the Centre and general information about the service users who attend and should not be given specific details about any individual.

Information on Computer and Manual Files
The Brothers of Charity Services need to ensure that all staff comply with the Data Protection Acts 1988 and 2003 which set out to protect the rights of privacy of the individual by imposing obligations on those who collect and store information on computer and in manual files. Staff must adhere to the eight rules of the Data Protection legislation as follows.

1. Obtain and process information fairly.
2. Keep it only for one or more specified, explicit and lawful purposes.
3. Use and disclose it only in ways compatible with these procedures.
4. Keep it safe and secure.
5. Keep it accurate, complete, and up-to-date.
6. Ensure that it is adequate, relevant and not excessive.
7. Retain it for no longer than is necessary for the purpose or purposes.
8. Give a copy of his/her personal data to that individual, or in the case of a child, his or her parent or guardian, on request.

Individuals have the right to have any inaccurate information held in these records corrected or erased [see website:www.dataprivacy.ie].

The Freedom of Information Acts 1997 and 2003 also give individuals similar rights. A service user, or parent, may choose to make application for relevant information from files or for a copy of all records using one of the following methods:

Administrative Access, or
Freedom of Information Acts 1997 and 2003.

Service users or parents are to be assisted and supported in any such application by staff in accordance with the *Procedures to be Followed in Dealing with Applications for a Service-User's File*.

Information held on computer file should be subject to the same controls as those held on manual files. The following guidelines should be adhered to.

1. Files opened containing personal information on an individual should always be filed under a password, thus preventing unauthorised access.
2. In addition to the above, there should be a "fast exit" button for use should some unauthorised person enter the area, or should the user have to leave the computer for a brief period.
3. Files should be deleted as soon as the information contained therein is deemed to have served its purpose.
4. Ensure information is kept accurate and up-to-date.
5. A policy should be drawn up regarding the setting up of data banks.
6. Information that is to go on files should be gathered from service users in an open and fair manner.
7. Information should only be used in ways compatible with the purpose for which the information was obtained in the first place.
8. These guidelines should be reviewed and up-dated on a regular basis.

Electronic Mail (E-mail)

1. When sending an e-mail where a service user's identity may need to be communicated to a colleague, only the service user's initials may be used. If a report or other correspondence containing confidential information is forwarded to a colleague or other appropriate individual such as a parent, via e-mail, it must be protected using a password. This practice is also required for the protection of confidential information stored on computers at source. A word document can be password-protected using the following method.

   Go to the icon named: File
   Click save as
   Click on Tools (top right hand corner of computer screen)
   Click on General Options
   Type in a password at Password to open the dialogue box
   A second screen comes up to confirm password- re-enter password
   The person receiving the document types in the password in order to open the word document.

2. To remove a password from a document, just delete the password from the dialogue box.

Video and Audio Taping

1. The reason the recording is being made, who will view it and the purpose to which it will be put must be explained in detail to the service user/family/advocate. They must be made fully aware that they are under no obligation to participate in such recordings.

2. Written consent, clearly stating the purpose for which the video or audio recording can be used, must be obtained from the service user/parent/advocate prior to the making of the recording.
3. Video and audio tapes of service users are subject to the same Agency Policy as those pertaining to files with regard to the storage and cataloguing of, access to, copying, and destruction of the recorded material.
4. The Freedom of Information Act and the Data Protection Act apply to video and audio recordings.

Photographs
When photographs of service users are taken for the purposes of publication, training, or display, written permission should be obtained from the service user, family or advocate for this purpose.

Data Bases
1. Health Board Data Base
   The Brothers of Charity Services are required by the Department of Health to maintain up-to-date records on service users. These records contain information on level of disability and future needs. Service users, parents or advocates should be made aware that this is occurring and should know what information is included on the data base. Service users, parents or advocates should be involved in completing the initial data base form and should be regularly informed of changes made.

2. Localised Data Bases
   With the widespread use of computers in the Service, it is possible that individual service communities will establish localised data bases. Individuals establishing such data bases are bound by the Data Protection Acts 1988, 2003, and must operate within the regulations of the Acts.

In addition, the following procedures should be adhered to regarding localised data bases.

1. A committee should be established to approve, monitor, and regulate such data bases.
2. An individual wishing to establish a data base must apply to do so to the above committee. The reasons for wishing to set up a data base, the individuals who will be included in the data base, and the purposes for which the data will be used must be furnished to the committee.
3. Only on approval of the committee can a data base be established.
4. Service users, advocates or families should be informed of the establishment of a data base and consent for an individual's inclusion should be obtained.

APPENDIX 1

I have read the Brothers of Charity Galway Services Policy on Confidentiality and I agree to abide by the principles contained therein.

SIGNED : .....……. DATE : .....

SIGNED : .....……. DATE : .....

Recommendations

1. All existing staff as well as new staff, trainees, and volunteers must be informed by their supervisors of the need to adhere to the Agency's Policy on Confidentiality.

2. The written Policy on Confidentiality should be distributed to all staff members, including temporary staff.

3. Every staff member as well as temporary staff, trainees, and y the Brothers of Charity Services Policy on Confidentiality. A sample of such a form is contained in Appendix 1 of this document. It is recommended that this form should be countersigned by their line manager.

4. More education and training should be provided for staff in both the area of recording confidential information and in the area of legal considerations.

5. Service users who are included as members of centre or service teams should be provided with appropriate training and support to ensure that they maintain confidentiality.

6. The Brothers of Charity Service needs to ensure that all staff comply with the Data Protection Acts 1988 and 2003.

7. Guidelines are required to govern how video and audio material are to be used so as to protect the right to privacy of an individual.

8. This Policy should be reviewed and up-dated every four years, initially June 2008.