APPROVED

Brothers of Charity Galway Services
Policy on Data Protection

Data Protection Acts 1988 and 2003

It is the policy of the Brothers of Charity Galway Services to comply with the obligations of the Data Protection Acts 1988 and 2003 and to ensure that all staff are aware of their data protection responsibilities.

The organization will maintain in place a Data Protection Monitoring Committee whose responsibilities will be to:

- Ensure compliance with Data Protection legislation,
- Have a clear procedure for handling requests for access to records,
- Ensure that appropriate procedures remain in place to support compliance including periodic review and audit, and
- Examine the case for the establishment of databases and regulate such databases.

Introduction

Data Protection is the safeguarding of the privacy rights of individuals in relation to the processing, storage and security of their personal data. Staff and service users supply information about themselves to the Brothers of Charity Services, and Data Protection legislation applies to this information. Data Protection law places obligations on the organization and all staff who keep personal information. Every individual has the right to know what personal information is held about him/her. The Act applies to living persons.

Data Protection rights apply whether the information is held:
in electronic format, for example, on computer,
in a manual or paper based form, or
in photographs and video images or digital images.

Manual files created before July, 2003 are not subject to the full application of the Acts until October 24, 2007 but those files are subject to access on request and security rulings apply to them.

[Pages 1-6 is the Policy on Data Protection; Pages 7-11 is Procedures and pages 12-14 are Guidelines for staff]

Signed: _____
Patrick McGinley, Director of Services

Date: 15th June, 2005

Policy No: 2005/04

Implementation Date: 15th July, 2005

The Principles of the Data Protection Act

Personal information should be:

1. Obtained and processed fairly, which means that the person providing it must know the purposes for which it will be used, and the persons to whom it will be disclosed;

2. Kept for specified, explicit and lawful purposes;

3. Used and disclosed only in ways compatible with these purposes;

4. Held securely;

5. Accurate, complete, up to date, and well organized;

6. Adequate, relevant, and not excessive; devoid of prejudicial, derogatory, malicious, vexatious, or irrelevant statements about the individual;

7. Held no longer than is necessary for the purpose or purposes; and

8. Accessible to the individual or person acting on his or her behalf on a reasonable basis.

1.0 Obtain and Process Information Fairly

At the time the personal data is being collected the person must be made aware of:

- What information is being collected
- Why the information is being collected
- Who within the agency will have access to the information
- How the information will be used
- The consequences of not providing the information
- What third party disclosures are contemplated
- The fact that there is a statutory obligation to collect the information
- That he or she can have access to the information, once collected, and
- The identity of the organization collecting the information.

The person must have given consent to the processing of the data. Processing means performing any operation or set of operations on data, including: obtaining, recording or keeping data, collecting, organizing, storing, altering or adapting the data; retrieving, consulting or using the data; disclosing the data by transmitting, disseminating or otherwise making it available; aligning, combining, blocking, erasing, or destroying the data. However there may be some situations where processing of data may be necessary without the explicit consent of the person having been obtained:

- compliance with a legal obligation;
- protecting the vital interests of the person where the seeking of the consent of the person is likely to result in those interests being damaged;
- preventing injury to, or damage to the health, of another person; and

- for obtaining legal advice, or in connection with legal proceedings, or is necessary for purposes of establishing, exercising, or defending legal rights.

2.0 Specified, explicit and lawful purposes

- Personal data can be obtained and kept only for purposes that are specific, lawful and clearly stated.

- The data should only be processed in a manner compatible with these purposes.

- An individual has a right to question the purpose for which the data is held, and the organization must be able to identify that purpose.

- The purpose for which the data was obtained cannot be expanded without reverting to the individual for further consent.

- A person is entitled to a full explanation of the logic used in any automated decision-making process where the decision significantly affects that person.

- The organization will identify the different sets and categories of data held and the specific purpose of each.

3.0 Use and Disclosure

Personal information should be used or disclosed only for the purpose for which it was obtained. However in certain restricted situations information can be used or disclosed for a purpose other than for which it was obtained:

- The person has explicitly consented to the proposed use or disclosure,
- The organization reasonably believes that the use or disclosure is necessary to lessen or prevent a serious and imminent threat to the health, safety or life of the individual, or a serious threat to public health or public safety,
- The use or disclosure is required or authorized by law, or
- The information concerns a person who is incapable of giving consent, and is disclosed to somebody who is responsible for that person to enable appropriate care or treatment to be provided. However, any disclosure to a third party should be limited to that which is either authorized or required in order to achieve the desired objective.

4.0 Held securely

Appropriate security measures must be in place to prevent unauthorized access to, or alteration to, disclosure, or destruction of the data, and against accidental loss or destruction.

- Access to information is restricted to authorized staff on a “need-to-know” basis in accordance with the Confidentiality and Files Policies.
- Computer systems must be password protected.

- Information held on computers must always be protected by a password to prevent unauthorized access.
- There must be back-up procedures in operation for computer-held data, including off-site back-up.
- Personal information on computer screens should only be visible to the computer user who must have the authority to access the information
- Staff must be aware of the organization's confidentiality and security policies and procedures and comply with them.
- Data must be securely disposed of when no longer required, or when the purpose for which the information was obtained is no longer current, relevant or valid.
- Premises must be secure when unoccupied, and personal information should be securely locked away when not in use.

5.0 Accurate, complete, up-to-date, well organized

Administrative and computer procedures must be adequate to ensure high levels of data accuracy and maintenance.

Personal information must be accurate. It is the responsibility of all staff who obtain or hold information to ensure that it is accurate, up-to-date and complete.

If information is inaccurate, each person has the right to have that information corrected, or erased, and the right to ask why the information is being held.

The manner in which information is recorded must comply with best practice models and it is the responsibility of managers to ensure that this is so.

6.0 Adequate, relevant, and not excessive

Only the information necessary to provide the support or services should be obtained/held.

Information held must be:

- Adequate in relation to the purpose for which it is held,
- Relevant in relation to the purpose for which it is held, and
- Not excessive in relation to the purpose for which it is held.

Information is obtained/held to:

- form a basis for planning or for providing a service,
- assist continuity of care amongst professionals,
- provide written evidence of a service,
- meet legal, professional, statutory or financial requirements, or
- provide information for clinical management, resource management, evaluation, clinical audit, quality assurance, or research.

7.0 Retention

Information should be held for the length of time the purpose for which it was obtained is valid.

Once the specific purpose for which the information was obtained is no longer current or valid, the information must not continue to be held and must be disposed of in a secure manner.

There must be clear and defendable reasons for retaining information longer than the retention time warranted by the specific purpose.

Notwithstanding the above, the retention of records must comply with any legislation relevant to the area of function. Such legislation relates to:

- The Child Care (Placement of Children in Residential Care) Regulations 1995. The records of children who are, or have been in care, under the provisions of the Child Care Act 1991, on either a voluntary basis or under a Court Order, must be kept in perpetuity;

- Medical, dietetics, nursing, occupational therapy, psychological, speech and language therapy, social work and all other therapies or treatments that service users receive within the Brothers of Charity Services where the recommended retention period is 8 years after death. (*Policy for Health Boards on Record Retention Periods,* 1999);

- Mental Health records: the recommended retention period is 20 years after cessation of treatment or 8 years after the service user's death if the service user died while still receiving treatment;

- Human Resources: Retention of records in Human Resources is subject to the relevant legislation. The Terms of Employment (Information) Act 1994. The Organization of Working Time Act 1997. Safety, Health & Welfare at Work (General Application) Regulations 1994 and Workers Protection (Regular Part-Time Employees) Act 1991 (See Guidance on Records Retention, National Federation of Voluntary Bodies, February 2000); and

- Financial Records: In accordance with Companies Act 1963: Six years plus one year (See Guidance on Records Retention, National Federation of Voluntary Bodies, February 2000)

8.0 Access

A person about whom personal data is held is entitled to:

- A copy of the data held about him/her
- Know the purpose for processing his/her data
- Know the identity of those to whom the data may be disclosed
- Know the source of the data, unless it is contrary to public interest
- Know the logic involved in automated decisions, and

- Have a copy of any data held in the form of opinions, except where such opinions were given in confidence.

However, right of access can be refused if:
- Providing access will pose a serious threat to the life or health of any individual, including the requester,
- Providing access would have an unacceptable impact on the privacy of other individuals, or
- It is required or authorized by law.

Requests for access to information held must be:
- In writing, and
- State that the request is being made under the Data Protection Act.

In response to a request for access to information the organization must:
- Supply the information to the requester promptly and within forty days of receiving the request, and
- Provide the information in a form which will be clear to the person, for example, any codes must be explained.

Procedure for dealing with a request under the Data Protection Acts 1988 & 2003

From July 1, 2003, manual records fall within the access regime outlined in the Data Protection Acts, 1988 & 2003.

1. When a Data Protection (DP) Request arrives

Data Protection requests are to be handled by the existing FOI Decision Makers. All Data Protection requests must be logged with the FOI Officer. When a Data Protection request arrives in a centre, it is to be forwarded immediately to the FOI Officer at Woodlands Centre.

Upon receipt of the DP request the FOI Officer will do the following.

I. Check that access is possible using the Data Protection Act. If not, the requester will be advised of their rights to seek access under the Freedom of Information Act.
II. Date stamp the request; this will be Day 1 of the request.
III. Open a file for the request.
IV. Document the discussion which leads to the Data Protection Request in its current form, if any.
V. Enter on the file the deadline for the decision – that is 40 calendar days from date of receipt.
VI. Check that the request comes within the scope of the Act namely that,
    - it was received in writing,
    - some reference is made to the Data Protection Act,
    - contains sufficient information to identify the records being sought, and
    - as the request refers to personal information ensure that the Requester has appropriate identification to establish who they are. In the case of personal information relating to third party requests, appropriate, current and satisfactory authorisation should be included.

2. Letter of acknowledgement to the Requester

The Data Protection Act does not prescribe a letter of acknowledgment. However, in keeping with best practice, the FOI Officer will write to the Requester:

- Acknowledging receipt of the request within 1 week
- Acknowledging receipt of the fee (€6.35)
- Including the name of the Decision Maker
- Verifying the date the decision is due, and
- Enclosing a copy of the Requester's Right of Complaint to the Data Protection Commissioner.

3. If Insufficient Information to identify the Records Requested

- After investigation, if it becomes clear that there is insufficient information to identify the records involved, the FOI Officer should contact the Requester, preferably by phone, fax or e-mail in order to clarify the request.
- The FOI Officer will inform the Requester that the request will be suspended until clarification is received.
- If, having offered all reasonable assistance, the request remains too vague the Brothers of Charity Services can refuse to process the request. All steps taken in attempting to process it will be clearly documented.
- The FOI Officer will notify the Requester of this decision in such circumstances.

4. Once the authenticity of the request is established, the FOI Officer will arrange with the Files Administrator for the assembling of all records covered by the request. The Files Administrator will:

- Identify all records both computer and manual which contain information (records) concerning the subject of the request.
- Initiate a search for documents/records stored on the PC network and other IT media, if applicable. All such documents held in an IT environment should be printed and should be entered chronologically in the file, including letters held in word processing software.
- Source and retrieve all manual records covered by the request.
- Aim to complete this work within 10 working days from the time the request has been received by the Services.
- Although there are no provisions for further charges in relation to search and retrieval, the Files Administrator shall document:
  - the effort involved in finding the records,
  - the locations searched,
  - names of those contacted with regard to sourcing files,
  - outcome of any discussions, and
  - details of hours involved.

Once all the records have been assembled the Files Administrator should have the following tasks carried out.

- Number all pages chronologically (including 'post-its' and complimentary slips), beginning at the back of the file with record number 1.
- Numbers should be written in the top right hand corner using a black ball point pen.
- Complete a 'Schedule of Records' to show the number of pages being released to the requester. This schedule will include a column where the Decision Maker will later identify the reasons if access to a record or a portion of a record is being refused.
- Make a complete copy of the records.
- The Decision Maker now takes over and begins the reviewing process.

5. Preparing Records for Access

Every reasonable attempt should be made by the Brothers of Charity Services to suit the individual's wishes regarding access. Normally, requesters seek a copy of the records and these should be issued by registered post. From time to time special needs are likely to arise and the Decision Maker should, where possible, agree the form of access. Special consideration should be shown to individuals with special needs.

Material, which is considered to be non-disclosable under the Act, should be blanked out using special editing tape.

6. Records which relate to a Third Party

Having reviewed the relevant records the Decision Maker must identify the records, which include the personal information of any person other than the requester. This information cannot be released to the requester without the consent of the "data subject" – see definitions. The usual procedure will be to blank it out.

7. Restriction of Right of Access

Individuals have a strong right of access to see their personal data. However, section 5 of the Data Protection Act provides that individuals do not have a right to see information relating to them where any of the following circumstances apply:

- If the information concerns an estimate of damages or compensation in respect of a claim against the Brothers of Charity Services, where granting the right of access would be likely to harm the interests of the organisation,
- If the information would be subject to legal professional privilege in court,
- If the information is kept only for the purpose of statistics or carrying out research, but only where the information is not disclosed to anyone else, and where the results of the statistical work or research are not made available in a form that identifies any of the individuals involved, or
- If the information is back-up data.

8. Restrictions on access to medical data and social work data

The Data Protection (Access Modification) (Health) Regulations, 1989 (S.I. no. 82 of 1989) provide that health data relating to an individual should not be made available to the individual, in response to an access request, if that would be likely to cause serious harm to the physical or mental health of the data subject. A person who is not a health professional should not disclose health data to an individual without first consulting the individual's own doctor, or some other suitably qualified health professional.

9. Internal Consultation

When a request is received for a file which contains records of a service user under the care of a health professional such as a Medical or Psychiatric Consultant, Psychologist, or a Social Worker, the Decision Maker shall consult, if necessary, with the relevant professional.

If a professional certifies that release of the information would be damaging to the requester, the Decision Maker must refuse release. There are no provisions for alternate access as in the case of FOI requests.

10. Right of Complaint to the Data Protection Commissioner

While there is no provision for Internal Review of the decision of the Brothers of Charity Services, any person may complain to the Data Protection Commissioner about the way their request was handled or any other matter. The Commissioner's address is:

Block 6,
Irish Life Centre,
Lower Abbey St.,
Dublin, 1.

Glossary of Terms

As with any legislation, certain terms have particular meaning. The following are some important definitions.

Data means information in a form, which can be processed. It now includes both automated data and manual data. However, the application of certain parts of the Act to existing manual data is deferred until October 2007.

Automated data means, broadly speaking, any information on computer, or information recorded with the intention of putting it on computer.

Manual data means information that is kept as part of a relevant filing system, or with the intention that it should form part of a relevant filing system.

Relevant filing system means any set of information that, while not computerised, is structured by reference to individuals, or by reference to criteria relating to individuals, so that specific information relating to a particular individual is readily accessible.

Personal data means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller

Processing means performing any operation or set of operations on data, including:

- obtaining, recording or keeping the data,
- collecting, organising, storing, altering or adapting the data,
- retrieving, consulting or using the data,
- disclosing the information or by transmitting, disseminating or otherwise making it available, and
- aligning, combining, blocking, erasing or destroying the data.

Data Subject is an individual who is the subject of personal data.

Data Controller is a person or entity who, either alone or with others, controls the contents and use of personal data.

Data Processor is a person who processes personal information on behalf of a data controller, but does not include an employee of a data controller who processes such data in the course of his/her employment.

Sensitive personal data relates to specific categories of data which are defined as data relating to a person's racial origin, political opinions, religious or other beliefs, physical or mental health, sexual life, criminal convictions or the alleged commission of an offence and trade union membership.

Data Protection Acts 1988 and 2003 Guidelines for Staff

Introduction

Data Protection is the safeguarding of the privacy rights of individuals in relation to the processing, storage and security of their personal data. Staff and service users supply information about themselves to the Brothers of Charity Services and Data Protection legislation applies to this information. Data Protection law places obligations on the organization and all staff who keep personal information. Every individual has the right to know what personal information is held about him/her. The Act applies to living persons.

Data Protection rights apply whether the information is held:

in electronic format, that is, on computer
in a manual or paper based form, or
in photographs and video images or digital images.

Manual files created before July, 2003 are not subject to the full application of the Acts until October 24, 2007 but those files are subject to access on request and security rulings apply to them.

The Principles of the Data Protection Act

Personal information should be:

1. Obtained and processed fairly, which means that the person providing it must know the purposes for which it will be used, and the persons to whom it will be disclosed;

2. Kept for specified, explicit and lawful purposes;

3. Used and disclosed only in ways compatible with these purposes;

4. Held securely;

5. Accurate, complete, up to date, and well organized;

6. Adequate, relevant, and not excessive. Devoid of prejudicial, derogatory, malicious, vexatious, or irrelevant statements about the individual;

7. Held no longer than is necessary for the purpose or purposes; and

8. Accessible to the individual or person acting on his or her behalf on a reasonable basis.

Staff Responsibilities relating to the Data Protection Act

The following applies to all forms of information – manual, electronic and paper. It refers to all files that are held – main and working files – all databases and all information collected, held, processed or stored.

Confidentiality
All staff are obliged to know and understand the Confidentiality Policy of the organization and to abide by its regulations and procedures.

When information is collected the individual must be informed about:

- Why the information is being collected,
- The uses for that information,
- Who will have access to the information,
- How the information will be stored,
- Who the information might be shared with and why, and
- That he or she can have access to the information and the process by which they can have access.

Information gathered/stored must be:

- Accurate, complete and up-to-date,
- Obtained and processed fairly,
- Kept only for one or more specified, explicit and lawful purposes,
- If the information is to be used for purposes other than for which it was obtained, the individual must be asked for further consent,
- Used and disclosed only in ways that are compatible with these purposes,
- Kept safe and secure,
- Adequate, relevant and not excessive in relation to the purpose for which it is held,
- Retained no longer than is necessary for the purpose or purposes, and
- Accessible to the person involved within the terms of access to records held under the Data Protection Act.

Information must be recorded according to best practice methodology

- Write in chronological order.
- Put the name and reference number of the service user on all records – each continuation sheet should have the name and reference number of the service user.
- Record factual information.
- Record opinions with a statement such as “In my opinion……..”
- Date all entries.
- Record contemporaneously.
- Write legibly – print if necessary.
- Use black ink (including diary entries which should not be in pencil).
- Do not leave blank spaces or skip lines.
- Put quotations in quotation marks.
- Sign each entry and state position.
- Give full name titles to all personnel mentioned in the record.

- As a general principal copies of reports should be given to the service user unless there are compelling reasons why this should not happen.

Mistaken entries

- Draw a line through a mistaken entry and initial it.
- Never use tippex/erasers.
- Do not obliterate entries.

Abbreviations

- Abbreviations must be kept to a minimum and if used should be in a standard form that is readily understood.
- Abbreviations should not be used in formal reports.
- Abbreviations should not be used in transfer/discharge documentation.

Retrospective Notes

- Notes made retrospectively should have the date the note was recorded and the date the entry referred to.

Security

- Information must be kept in a secure manner.
- Files should be kept in locked cabinets.
- Information held on computers should be password protected.
- Personal information on computer screens should only be visible to the computer user.
- Data must be securely disposed of when no longer required, or when the purpose for which the information was obtained is no longer current, relevant or valid.