Eist

Cancer Support Centre

Carlow

DATA PROTECTION

POLICY

TABLE OF CONTENTS

1. Policy Statement
2. Purpose of Data Protection Policy
3. Scope
4. Relevant Policies and Legislation
5. Glossary of Terms and Definitions
    - 5.1 Who does data protection apply to?
    - 5.2 What is data?
    - 5.3 What is data processing?
    - 5.4 Who is a data processor?
    - 5.5 Principles of data protection
    - 5.6 What is a data breach?
6. Roles and Responsibilities
7. Guidelines/Procedures
    - 7.1 Acquiring information
    - 7.2 Data recording
    - 7.3 Data storage
    - 7.4 Consent
    - 7.5 Access to data
    - 7.6 Third party data requests
    - 7.7 Data for research purposes
    - 7.8 Granting data requests
    - 7.9 Use of electronic equipment and mail
    - 7.10 Removing data from the premises
    - 7.11 Opting-out
    - 7.12 Disposal of records
    - 7.13 Breaches of data protection

8. Implementation plan

9. Review and audit of policy

10. References

Appendix 1 **6**

DATA PROTECTION POLICY

1. Policy Statement

Our organization, the Eist Cancer Support Centre, Carlow, is committed to respecting the rights of individuals and to their privacy and confidentiality. We are open and honest with individuals concerning the method by which data is processed. We will train and support staff and volunteers to support compliance with the Data Protection Acts

2. Purpose of Data Protection Policy

The purpose of the Eist Cancer Support Centre, Carlow, policy on data protection is to ensure compliance with the law and to ensure accountability and transparency in how data is handled and processed

It sets out an approach in the event of an information/data breach. Information/data breaches may occur because of deliberate acts of disclosure to unauthorised persons, accidental disclosure to unauthorised persons, and loss due to fire, storm or flood, possible theft (e.g. mobile storage devices or computers)

3. Scope

The policy applies to all employees, volunteers, members/clients and Board members

4. Relevant Policies and Legislation

- Data Protection Acts (1988 and 2003)
- European Communities Data Protection Regulations (2001)
- European Commission (Data Protection and Privacy in Telecommunications) Regulation (2002)
- Data Protection EU Directive 95/46/EC
- Criminal Damages Act (1991)
- Our organisation's policy on confidentiality

5. Glossary of Terms and Definitions

5.1 Who does data protection apply to?

Any data relating to a living individual whose identity can be discerned either from the data available or in conjunction with other relevant data which is held by the organization is regarded as personal data. Some personal data is also considered to be sensitive personal data. Sensitive personal data includes information regarding:

- Race or ethnicity
- Political opinions
- Religious or philosophical beliefs
- Trade union affiliations

- Physical/mental health
- Sexual orientation
- Commission of or alleged commission of an offence
- Date of birth
- PPS number

Other confidential information includes information with regard to the organization such as financial records, payroll data, personnel information and legal documents

5.2 What is data?

Data infers any information that can be processed. This includes information which is kept in a filing system (manual data) and information which is kept on computer (automated data)

5.3 What is data processing?

Data processing infers performing any operation or set of operations on the data, whether or not by automatic means. Processing includes: obtaining, recording and keeping data; collecting, organising and storing data; altering or adapting data; retrieving, consulting, using or disclosing data; transmitting or disseminating data; aligning, combining, blocking, erasing or destroying data. Our organisation is responsible for all personal data that it processes

5.4 Who is a data controller?

Under the Data Protection Acts, a data controller is defined as the individual or legal person in control of and responsible for the storing and use of personal information on computer or structured manual files. Our organisation controls and is responsible for all personal data that it holds

5.5 Principles of data protection

The core principles underpinning our policy on data protection states that confidential information and privacy are protected and data/information will not be released to third parties without the prior written consent of the person to whom the data applies. In addition, the principles that must be complied with under the Data Protection Acts with regard to personal information apply. These are:

- The information must be obtained and processed fairly
- It must only be kept for specified purposes and for lawful purposes
- It must be used and disclosed only in ways that are compatible with the purpose for which it was acquired initially or for which it was subsequently approved
- It must be kept safe and secure
- It must be accurate, complete and where necessary, up to date
- It must be adequate, relevant and not excessive, i.e. seek and retain only the minimum amount of personal data which is needed to achieve specified purposes

- It must not be retained for longer than is necessary for the specified purpose(s) and according to stated policies as they apply to different sources
- A copy of the information must be given to the individual to whom it relates at his/her request

5.6 What is a data breach?

A data breach is the intentional or unintentional disclosure or release, loss or theft of personal information/data

6. Roles and Responsibilities

It is the responsibility of the Service Manager to develop an appropriate policy on data protection

It is the responsibility of the Board of Management to approve the policy on data protection

It is the responsibility of the Service Manager to review and update the policy on data protection

It is the responsibility of all Board/management committee members, volunteers, staff, and individuals contracted by the organisation to be familiar with and to comply with the policy on data protection

All breaches of this policy must be reported to the Board of Management

It is the responsibility of the Board of Management to deal with any breach of the data protection policy

The organisation controls and is responsible for all personal data that it holds and is responsible for all personal data that it processes

7. Guidelines/Procedures

The following guidelines/procedures outline the steps to be taken in the Eist Cancer Support Centre, Carlow, in order to achieve the aims and goals as outlined in the purpose, scope and policy statement

7.1 Acquiring information

The person responsible for gathering information from an individual must make the individual aware of their identity and inform them of the purpose for gathering the data, whether or not it will be shared with third parties, how long it will be held for and whom they can contact if they wish to see a copy of their personal data

7.2 Data recording

Data that is recorded should be accurate and complete and should be entered into records in accordance with data protection guidelines

Corrections will be promptly made when inaccuracies, mistakes, misleading information or incomplete information is brought to light

7.3 Data storage

Adequate security measures are in place to protect the safety and integrity of data under the control of the Eist Cancer Support Centre, Carlow

Personal data that is no longer ‘live’ or current will be archived. Data will be kept in the archive for as long as appropriate for financial or legal reasons or if it is necessary for historical or statistical research

Duplicate records set up in error will be destroyed

Suitable back-up facilities, e.g. hard copy, off-site data servers, will be put in place to protect data in the event of disruption

7.4 Consent

Consent for the release of data regarding an individual must be sought from that individual

Such consent must be informed and active and given freely and remain unambiguous

The person responsible for providing the consent should present it in written form, e.g. by signing a consent form. If the consent is provided verbally, this should be recorded and should include the date of consent

A person has the right to withdraw their consent at any time. If consent is withdrawn, this, together with the date, should be recorded and acted upon accordingly

7.5 Access to data

Access to personal data by staff or volunteers will be provided on a ‘needs only’ basis in the execution of their roles and responsibilities

Requests for access to personal data made by the individual to whom the data pertains must be made in writing

Responses to such requests will be made within 10 days of receipt of such request

Before making a response to such a request the following criteria must be met:

- Is the data personal data?
- Is the person requesting the data the bona fide owner of the requested data?
- Does the data relate specifically to the individual?
- Are there any references to third parties that should be withheld?
- Has the request been made in writing?

Once a request is granted, this must be recorded on the file

7.6 Third party data requests

In general, access by third parties to personal information will be denied without the prior written consent of the individual to whom the personal data pertains

Exceptions to this are:

- Where discharge of a regulatory activity is required
- Where detection or prevention of a crime or the apprehension of an offender is involved
- Where abuse or self-harm are suspected

Such requests will be dealt with on a case-by-case basis

7.7 Data for research purposes

Only anonymised data will be made available by the organization, to third parties, for which it contracts to conduct research on its behalf. Such data will only be released following verification by the Board of Management which proves that the data does not contain any information that would allow direct identification of an individual (e.g. name, address, date of birth, etc.)

Confidential or personally identifiable information will only be released to third parties contracted by the organisation with the prior written consent of the individual. Such consent must be given without any duress or pressure. The individual must be made aware that they may withhold such consent or they may withdraw such consent at any time without any consequences. The individual must be given a contact name and number should they wish to discuss any aspect of the research, or concerns they may have, or if they wish to withdraw their consent

7.8 Granting data requests

Data requests may only be granted by the Board of Management

7.9 Use of electronic equipment and mail

Fax machines and computers must be positioned to minimize the risk of unauthorised individuals accessing them or viewing incoming messages or information on screen

Personal information held on computers, laptops or mobile computer devices should be password protected

Mobile phones which are used in the context of work which contain personal information must be protected by a Personal Identification Number (PIN)

If at all possible, personal information should only be transmitted by encrypted file via e-mail. Faxes of this type of information should be avoided

Mail containing sensitive personal information should always be marked as ‘Strictly Private and Confidential’ and the outside of the envelope should contain ‘return to sender’ information

7.10 Removing data from the premises

Transit of information outside the premises of the Eist Cancer Support Centre, Carlow, should only occur with the correct authorisation and should be kept to a minimum. Where it is necessary, all precautions must be taken to ensure the security of the information before, during and after transit

Laptops, portable mobile devices and /or files containing personal information or confidential organisational information should be locked securely in the boot of any car used for transportation and should not be left unattended in the car, especially overnight

7.11 Opting-out

Individuals have the right to opt-out of having their data used as a result of direct marketing or fund raising communications from the Eist Cancer Support Centre, Carlow

Such an opt-out option will be clearly identified in all marketing or fund raising communication. The process for opting-out will be clearly identified

7.12 Disposal of records

Disposal of records must maintain the confidentiality of the information contained in the records and avoid accidental loss or disclosure regarding the contents of the records

The approved method of destruction is shredding, either internally or by a third party approved by the manager

Authorisation for destruction of records must be obtained from the Board of Management. Records for destruction must be segregated from general waste

7.13 Breaches of data protection

Volunteers, staff, contracted third parties and Board members should report any information/data breach to the Service Manager at the earliest possible date

This person should record the details of the breach accurately and should include the following:

- Dates and times of the breach
- The individual that reported the breach and the date and time of recording
- Description of the breach and any corroborating materials, e.g. logs, error messages, etc.

The risks associated with the breach should be assessed on the basis of the type of

information/data which is involved, how sensitive the data is, relevant information which could be obtained by a third party, how many individuals are affected and what, if any, security measures were in place

Based on this information, an appropriate response will be developed, e.g. retrieval of the data if possible, notifying the individuals concerned, making an apology, notifying the Gardaí, ensuring that appropriate security measures are put in place (e.g. passwords, encryption, locks), disciplinary procedures, etc.

Deliberate breaches of confidentiality or disclosure of personal information/data to unauthorized persons will result in dismissal or termination of a contract

8. Implementation plan

The person responsible for rolling out, communicating and implementing this policy in the Eist Cancer Support Service is the Service Manager. The policy will be communicated and disseminated to staff, volunteers and contracted third parties such as counsellors and therapists in the following manner: Paper Copy

The following training will be provided to staff, volunteers and contracted third parties: Core Skills

9. Review and audit of policy

The policy on data protection will be reviewed by the Service Manager periodically and feedback will be provided to the Board/management committee, staff, and volunteers and contracted third parties

Any changes to the policy on data protection will be agreed by the Board/management committee and notified to staff, volunteers and contracted third parties

10. References

Irish Cancer Society (2010) Guidelines for Cancer Support Services in Ireland. Dublin: Irish Cancer Society

Appendix 1

Confidentiality Declaration

I understand that in the course of my duties with the Eist Cancer Support Centre, Carlow, in the event that I may come into possession of medical and personal information regarding clients or confidential information relating to other staff or volunteers. I understand that all such information must be treated with the strictest confidence and that I will not discuss or divulge this information to any individual that does not have the privilege to this information or without the expressed permission of the client involved

I understand that I may not remove any documents or items belonging to the Eist Cancer

Support Centre, Carlow, which contains any confidential information from the service's premises at any time without proper advanced authorization

I understand that if I breach confidentiality, I can be dismissed from my position or my volunteer contract can be terminated

I agree to return to the Eist Cancer Support Centre Carlow, upon request, and in any event, upon the termination of my volunteering period, all documents and items belonging to the service, which contains or refers to any confidential information which is in my possession or under my control. I understand that even when my volunteer role has elapsed with the Eist Cancer Support Centre, Carlow, I am bound to maintain all Information of a confidential nature regarding the service, its clients and staff and volunteers

I have read and understood the confidentiality policy of the Eist Cancer Support Centre, Carlow.

Signature: _____

Print Name: _____

Witnessed by designated representative of the Eist Cancer Support Centre, Carlow

Signature: _____

Print Name: _____

Date: _____