Carriglea Cáirde Services

Carriglea, Dungarvan, Co. Waterford.
T 058 41322 F 058 41432
E info@carrigleaservices.com

SD-25

POLICY AND PROCEDURE

Information Governance, Confidentiality, Data Protection and Freedom of Information

Approved by: _____

Date Effective From: 17-4-2017

Review Date: April 2020

CARRIGLEA CAIRDE SERVICES

Procedures Manual

Title: INFORMATION GOVERNANCE - CONFIDENTIALITY DATA PROTECTION AND FREEDOM OF INFORMATION

1.0 Scope

1.0 To ensure good information governance, confidentiality and access to records.

2.0 Aims and Values

2.1 To ensure that information is stored and accessed in a way, which complies with the Data Protection Act 1988 & 2003, the Freedom of Information Act, 2014 and any subsequent legislation that relates to information held and the rights of the individual to access it.

2.2 To make this procedure available to all staff and service users.

2.3 To ensure that staff and service users' confidentiality is respected.

3.0 Contents

4.0 Referenced Documents

HR-09 E-mail and Internet Policy
SD-38 Record Keeping and Records Management Policy
SD-10 CCTV Surveillance
Data Protection Act 1988 & 2003
Freedom of Information Act, 2014

5.0 Responsibilities

5.1 Management and all staff.

6.0 CONFIDENTIALITY

6.1 All staff are obliged to maintain confidentiality. Staff are likely to have access to or hear information concerning the medical or personal affairs of service users or other staff, or other sensitive information in relation to the Services. Staff are forbidden to give information or to discuss the service users or the business of the Services outside of their area of work or to disclose information to anybody who is not authorised to have such information. Agreement to maintain confidentiality is included in the terms and conditions of employment of all staff.

- Managers are responsible for identifying information which is classed as 'confidential' within the service.
- Information marked 'confidential' should not be shown to any person who is not on the document distribution list.
- Reproduction/photocopying of such documents should only be carried out following appropriate authorisation.
- Confidential information should not normally be sent via e-mail or Fax unless the recipient can ensure security on receipt.
- Staff should be aware that non-employees are not bound by the confidentiality rules of the services and therefore care needs to be exercised in sharing information with anybody outside of the services.

7.0 DATA PROTECTION

7.1 **Data Protection Acts 1988 and 2003**
It is the policy of Carriglea Cáirde 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. Carriglea Cáirde Services is registered with the Data Protection Commissioner to hold personal information.

7.2 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 Services and Data Protection legislation applies to this information. Data Protection law places obligations on the Organisation 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.

7.3 Data Protection rights apply whether the information is held:

- in electronic format, for example, on computer, i-phone, memory key,
- in a manual or paper based form,
- in photographs and video images or digital images.

7.4 Recognisable images captured on CCTV systems are personal data and are subject to the provisions of the Data Protection Act. See Policy & Procedure on *CCTV Surveillance.*

8.0 THE PRINCIPLES OF THE DATA PROTECTION ACT:

8.1 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 or outside of 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
- If there is a statutory obligation to collect the information
- That he/she can have access to the information, once collected

The person must have given consent to the processing of the data.

8.2 Specified, explicit and lawful purposes

- Personal data can be obtained, processed and kept only for purposes that are specific, lawful and clearly stated.
- An individual has a right to question the purpose for which the data is held, and the Organisation 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.

8.3 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 Organisation 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 authorised by law,
- 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 authorised or required in order to achieve the desired objective.

8.4 Held securely

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

- Access to information is restricted to authorised staff on a "need-to-know" basis.
- Computer systems and information held on computers must always be protected by a password to prevent unauthorised 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 organisation'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.

8.5 Accurate, complete, up-to-date, well organised

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

- 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.

8.6 Adequate, relevant, and not excessive

Only the information necessary to provide support or services should be obtained/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,
- provide information for clinical management, resource management, evaluation, clinical audit, quality assurance, or research.

8.7 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 should 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 and with Carriglea Cáirde Services *Record Keeping and Records Management Policy.*

8.8 Access

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

- A copy of the data held about him/her
- 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,
- It is required by law.

Requests for access to information held must be:

- In writing,
- State that the request is being made under the Data Protection Act.

In response to a request for access to information the Organisation must:

- Supply the information to the requester promptly and within forty days of receiving the request,
- Provide the information in a form which will be clear to the person – e.g. any codes must be explained.

Data Protection requests are to be handled by the FOI Decision Maker.

Any person may complain to the Data Protection Commissioner about the way their request for access to information was handled.

9.0 STAFF RESPONSIBILITIES RELATING TO PORTABLE ELECTRONIC DEVICES

- Staff are responsible for the safety and security of laptops and other mobile electronic devices (e.g. USB keys) in their possession. Staff must ensure that no unauthorised person can access the personal information that is held on laptops and mobile devices.

- Those who supervise students on placement in the Services must ensure that no identifiable personal information relating to service users or families will be placed on laptops or mobile devices belonging to the students.

- It is the sole responsibility of the laptop user to store it safely. Laptops are not to be carried in cars unless they are placed in the locked boot of the car and must not be left overnight in a car.

- When a laptop is kept at staff member's residence, it must be kept out of sight for protection against theft. If using a laptop at home, information must not be visible to any other member of the household.

- Where possible, laptops should be placed in a locked filing cabinet in offices.
- For security reasons, laptops and USB keys should be encrypted.

In the event of a breach of data security, staff must inform the Chief Executive immediately.

This policy should be read in conjunction with the HR policy on *E-mail and the Internet (HR-09).*

10.0 FREEDOM OF INFORMATION (FOI)

Carriglea Cáirde Services is subject to the terms Freedom of Information Act, 2014 and any further amendments. However, access to the greatest extent possible will be allowed to the organisation's records and information without resort to the procedures under the Freedom of Information Act.

The Services promotes openness and accountability in allowing service users access to their own personal information and staff access in relation to their personnel records. Any application for access to files which is not submitted strictly under the Freedom of Information Act 2014 is referred to as a request for Administrative Access. Requests for Administrative Access are to be welcomed and those choosing this route are to be helped and supported at every stage in being given appropriate access to the relevant information which they require. Requests for Administrative Access should only be dealt with by senior members of staff.

It must be noted that when giving/showing details to a person in relation to their own personal information, care needs to be taken to ensure that the document does not contain any personal information in relation to another person.

All staff should be aware that any record, notes, messages, memo's, entries in work diaries, e-mails, etc. that they create could be subject to release under FOI and therefore great care should be taken that the content of any data maintains the dignity of the subject of the record.

The Act asserts the right of members of the public to obtain access to official information to the greatest extent possible consistent with the public interest and the right to privacy.

Under the terms of the FOI Act, every individual should have the right to:

- know what information is held in the services records about him/her, subject to certain exemptions to protect key interests;
- have inaccurate personal material on file corrected;
- obtain the reasons for a decision which affects them personally

Under the Freedom of Information, Model Publication Scheme published in October, 2015, Carriglea Cáirde Services will publish the following information on its web-site:

- Information about the Services
- Services provided
- Decision making process for major policy proposals.
- Financial information
- Procurement
- Details of FOI disclosures in relation to non-personal requests

11.0 MAKING AN FOI REQUEST

A person who wishes to exercise their right of access to records under the Act can make a request, in writing, to the Chief Executive to access to the record concerned:

- stating that the request is made under the FOI Act
- setting out sufficient particulars to enable the record to be identified
- specifying the preferred form of access, if he or she has such a preference (e.g. inspection of the originals, photocopy, etc.).
- making payment of any fees prescribed in regulations. A request for records containing only personal information related to the requester (including a request

made by a parent or guardian on behalf of a minor or disabled person or the next of-kin or personal-representative on behalf of a deceased person) is exempt from this fee.

All requests made under the FOI Act will be passed the Services Decision Maker who will decide whether or not information can be released bearing in mind the requirements of the Act to protect confidentiality, privacy and the public interest.

Health Professionals Records

When a request for access to medical records is received, it is regarded as good practice that the application is discussed with the treating health professional.