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: 29th March, 2019

Review Date: March, 2022

CARRIGLEA CAIRDE SERVICES

Procedures Manual

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

1.0 Scope

1.0 The policy applies to all staff, former employees, volunteers, agency workers, of Carriglea Cáirde Services and students on placement.

2.0 Aims and Values

2.1 To ensure high standards in information governance.

2.2 To ensure that information is obtained, processed, stored and accessed in a way, which complies with the General Data Protection Regulation (GDPR), Irish data protection law, the Freedom of Information Act, 2014 and any subsequent legislation that relates to personal information held and the rights of the individual to access it.

2.2 To make this procedure known to all stakeholders, including staff, service users and any person whose personal data is held by the Services.

2.3 To ensure that staff and service users' confidentiality is respected and that sensitive information relating to the business of the Services is protected.

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
C4-90	Consent Form for use of photographs/images
C4-44	Notice of Property Incident
C4-92	Data Breach Incident Form
C4-93	Data Subject Access Request Form
	General Data Protection Regulations
	Freedom of Information Act, 2014

5.0 Responsibilities

5.1 Management and all staff.

6.0 POLICY STATEMENT

6.1 Carriglea Cáirde Services needs to collect and hold personal information to effectively carry out the everyday business functions and activities of the services. Such data is collected from applicants for services, employees, ex-employees, service users, volunteers, contractors, suppliers and board members. Information which is collected includes, but is not limited to, name, address, email address, data of birth, photograph, IP address, PPS and other identification numbers, private and confidential information, sensitive information and bank/credit card details.

In addition, the Services may be required to collect and use certain types of personal information to comply with the requirements of the law/regulations. However the Services is committed to processing all personal information in accordance with the ***General Data Protection Regulation (GDPR)*** and any other relevant data protection laws and codes of conduct.

6.2 The purpose of this policy is to ensure that the Services meets its legal, statutory and regulatory requirements under the data protection laws and to ensure that all personal and special category information is processed compliantly and in the individuals best interest.

Data protection laws include provisions that promote accountability and governance and as such the Services has put comprehensive and effective governance measures in place to meet these provisions. The aim of such measures is to ultimately minimise the risk of breaches and uphold the protection of personal data.

6.3 All staff are obliged to make themselves familiar with the provisions of this policy and procedure and to abide by its provisions.

6.4 Carriglea Cáirde Services does not undertake automated decision-making or profiling.

7.0 CONFIDENTIALITY

7.1 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 fellow 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.

7.1.1 Confidential information should not be shared with to any person who is not authorized to have such information.

7.1.2 Reproduction/photocopying of confidential documents should only be carried out following appropriate authorisation.

7.1.3 Confidential information should not be sent via e-mail or fax unless the recipient can ensure security on receipt.

7.1.4 Incoming and outgoing postal correspondence is held in a secure area while awaiting collection/distribution.

7.1.5 When a request for information is made over the telephone, staff must verify the identity of the person, before sharing any personal information.

7.1.6 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 personnel.

7.1.7 Access to offices and the archive rooms is limited to staff who require access for business purposes.

8.0 DATA PROTECTION

8.1 **General Data Protection Regulation (GDPR):** The General Data Protection Regulation (GDPR) applies to all EU Member States since 25th May 2018. Its rules replace existing Irish data protection laws. Carriglea Cáirde Services is obligated under the GDPR to protect personal information, and to obtain, use, process, store and destroy it, only in compliance with its rules and principles.

8.2 **Personal Data:** Information protected under the GDPR is known as *"personal data"* and is defined as: -

"Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

The Services ensures that a high level of care is afforded to more sensitive personal data falling within the GDPR's **'Special categories of Personal Data'** which include *"personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"*.

Further information on what constitutes personal information and your rights under the GDPR can be found at www.dataprotection.ie.

8.3 **The Office of the Data Protection Commissioner (DPC):** The DPC is an independent regulatory office whose role it is to uphold information rights in the public interest and they can issue enforcement notices and fines for breaches in any of the Regulations, Acts or Laws regulated by them.

Carriglea Cáirde Services is registered with the Data Protection Commissioner to hold personal information.

8.4 **Data Protection Officer:** Carriglea. Cáirde Services is obliged to appoint a Data Protection Officer (DPO). Ms. Mary McGrath, Administrator/Quality & Standards Manager, has been appointed to this role.

All requests for information under the Data Protection Act are to be referred to the Chief Executive or to the DPO.

The DPO must be informed immediately of any data breach.

The DPO will report breaches as necessary to the Office of the Data Protection Commissioner.

The DPO will arrange for regular data protection audits to be carried out.

9.0 GDPR PRINCIPLES

9.1 Article 5 of the GDPR requires that personal data shall be: -

a) Processed lawfully, fairly and in a transparent manner in relation to the data subject ***('lawfulness, fairness and transparency')***

b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; ***('purpose limitation')***

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which the data is processed ***('data minimisation')***

d) Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that inaccurate data is rectified without delay ***('accuracy')***

e) Kept for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods if the data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to safeguarding the rights of the data subject ***('storage limitation')***

f) Processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. ***('integrity and confidentiality').***

Article 5(2) requires that *'the controller shall be responsible for, and be able to demonstrate, compliance with the data protection laws principles'* ***('accountability')***.

9.2 Legal Basis for Processing *(Lawfulness)*

Prior to carrying out any personal data processing activity Carriglea Cáirde Services identifies and establishes the legal basis for doing so.

The legal basis is documented on the Services data processing log and Privacy Notice.

Data is only obtained, processed or stored where: -

a. The data subject has given **consent** to the processing of their personal data for one or more specific purposes
b. Processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps prior to entering into a contract
c. Processing is necessary for **compliance with a legal obligation** to which the Services is subject
d. Processing is necessary in order to **protect the vital interests** of the data subject or of another natural person

e. Processing is necessary for the performance of a task carried out **in the public interest** or in the exercise of official authority vested in the Services

f. Processing is necessary for the purposes of the **legitimate interests** of the Services

9.3 Processing Special Category Data

The Services only processes personal information classed as special category or information relating to criminal convictions where: -

a. The data subject has given **explicit consent** to the processing of the personal data

b. Processing is necessary for the purposes of carrying out obligations and exercising specific rights of the controller or of the data subject with regard to **employment, social security or social protection law**

c. Processing is necessary **to protect the vital interests** of the data subject or of another natural person where the data subject is incapable of giving consent

d. Processing is carried out in the course of the **Services legitimate activities** with appropriate safeguards (*except where such interests are overridden by the interests or fundamental rights of the data subject).*

e. Processing relates to personal data which are **manifestly made public** by the data subject

f. Processing is necessary for the establishment, exercise or defense of **legal claims**

g. Processing is necessary for reasons of **substantial public interest** or public interest in the area of public health

h. Processing is necessary for the purposes of **preventive or occupational medicine**, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services

i. Processing is necessary for **archiving purposes** in the public interest, scientific or historical research purposes or statistical purposes.

10.0 GOVERNANCE PROCEDURES

10.1 **Privacy by Design:** Carriglea Cáirde Services operates a *'Privacy by Design'* approach and ethos. This means that processes are designed from the outset to protect the rights of data subjects**.** The controls and measures detailed below, support this ethos.

10.1.1 **Data Minimisation:** The Services only obtain, retain, process and share data that is essential for carrying out its services and/or meeting its legal obligations and only retains data for as long as is necessary.

Measures to ensure that only necessary data is collected includes: -

a. Forms and surveys only have the fields/questions that are relevant to the intended purpose.
b. Information requested during face-to-face or telephone conversations should be relevant and necessary
c. Agreements are in place with third-party controllers/processors with whom personal information is shared which state that only relevant and necessary data is processed and also that personal data is secure from data breaches.

10.1.2 **Pseudonymisation:** The Services uses pseudonymisation where possible to record and store

personal data in a way that ensures it can no longer be attributed to a specific person without the use of separate, additional information (*personal identifiers*) e.g. NASS numbers or HIQA ID numbers.

10.1.3 **Encryption:** The Services aims to use encryption as a risk prevention measure for securing personal data.

10.1.4 **Restriction:** Restricting access forms part of the Services processes, systems and structure and ensures that only those with authorisation and/or a relevant purpose have access to personal information.

10.1.5 **Hard Copy Data:** The Services obtains, processes and shares personal information in paper format (*e.g. service user records, invoices*). When sharing such data the Services will:

a. If applicable redact information to ensure that only the relevant information remains (*i.e. when the personal data is being passed to a third-party for processing and not directly to the data subject*).

b. When using electronic formats to send information to a recipient e.g. scanning/e-mailing, ensure that secure methods are applied and ensure that any scanned document is deleted from the scanning equipment immediately.

c. The identity and contact details of intended recipients are checked before sending any personal information.

10.2 **Data Processing Log:** The Services maintains a log of all processing activity.

10.3 **Data Protection rights apply whether the information is held:**

a. in electronic format, for example, on computer/lap-top, smart-phone, memory key,

b. in a manual / paper based form,

c. in photographs and video images or digital images. Service users are requested to give written consent for their photograph to be published in newspapers, brochures, on notice boards or on the Services website. Consent must also be obtained before making video recordings. Consent is given by signing a *Consent Form for Photographs/Images.*

d. In the event that photography or video images of a service users is recommended by a clinician to be of benefit to the service user for clinical recording purposes (e.g. video recording of epileptic seizures or photographs of skin conditions), the permission of the service user must be obtained. Also a senior manager and the service user's family must be consulted with before any such photograph or video recording is taken. A Data sharing agreement will be put in place with any clinician who requests to be given a copy of a video recording or photograph taken for clinical reasons.

10.4 Recognisable images captured on CCTV systems are personal data and are subject to the provisions of the GDPR. See Policy & Procedure on *CCTV Surveillance.*

10.5 **Third-Party Processors:** The Services uses external processors for certain processing activities. The Services identifies all personal data that is processed outside of the Services, so that the processing activity, processor and legal basis are all recorded, reviewed and easily accessible. *Such external processing includes but is not limited to:*

a. IT Systems and Services

b. Legal/Auditing Services

c. Human Resources/Garda Vetting

d. Payroll/Pensions
e. Accounts
f. Hosting of Email facilities

Strict due diligence procedures are in place to assess all processors prior to forming a business relationship. Service Level Agreements / contracts with each processor are put in place.

11.0 DATA PROTECTION IMPACT ASSESSMENT (DPIA)

11.1 Data Protection Impact Assessments are a requirement of the GDPR. Where the Services is considering carrying out processing that utilises new technologies, and/or where there is a likelihood that such processing could result in a high risk to the rights of data subjects, a Data Protection Impact Assessment (DPIA) is carried out. This allows assessment of the impact and risk before carrying out the processing, thus identifying and correcting issues at source and reducing risks and the likelihood of breaches.

11.2 The DPIA is carried out by a team which will include the Data Protection Officer. Where the system involves new technologies, the DPIA team will include an IT representative.

11.3 Further information regarding the requirement for a DPIA is available from the Office of the Data Protection Commissioner

12.0 DATA SECURITY

12.1 Carriglea Cáirde Services is committed to the protection of information and data which is stored in physical and electronic format.

12.2 Responsibilities relating to Electronic Devices:

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

b. Those who supervise students on placement in the Services must ensure that the students are informed not to record identifiable personal information relating to service users, families or staff on documentation relating to their studies or research.

c. It is the sole responsibility of a laptop user to store the equipment safely.

d. When a laptop is kept at a 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.

e. Where possible, laptops should be placed in a locked filing cabinet in offices.

f. Laptops, external hard drives and USB keys should be encrypted.

g. Computer and lap-top screens must be set to log off after a short period of inactivity. This period may be between one minute and ten minutes depending on the business needs of the area.

h. Devices, including smart-phones must be suitably password protected and staff must not share passwords or write passwords on the device or in any place where they can be identified.

i. Staff should not access or edit data using another person's access code.

j. Special Category Data relating to data subjects should not be stored on smart-phones.

k. No electronic device on which data is stored should be disposed of without all data first being effectively and fully deleted from the device.

l. If an electronic device on which data is stored is re-allocated to another department or staff members, any personal data which is not required by that person or department must be deleted before the device is re-allocated.

m. The Services keeps a log of all computers and portable electronic devices and the location/names of the person to which they are assigned.

n. Adequate and effective firewalls malware and anti-virus applications must be running and maintained on all the services computers, servers and lap-tops.

In the event of a breach of data security, e.g. loss of or unauthorised access to a computer, lap-top, USB key, smart-phone, or paper files, accidental transfer of personal/confidential to an unauthorised person or unintentional deletion of data, staff must inform their manager and the Data Protection Officer immediately. A Property Incident Form must also be completed.

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

12.3 <u>Remote Access:</u>

a. Remote access refers to any work that takes place off-site using the Services information. It includes working from home and taking personal information off-site

b. It is the responsibility of all employees with remote access privileges to the Services information, to use their devices in an ethical manner at all times and to ensure that their remote access connection is given the same consideration as the on-site connection.

c. Employees must not work on company business remotely or take personal information relating to the Services, its service users or employees off-site without the permission of a senior manager.

13.0 PAPER RECORDS

13.1 Staff should not leave personal or sensitive information in any area where it may be seen or accessed by an unauthorised person. This includes ensuring that any documents stored on office desks cannot be seen by anybody visiting the office.

13.2 Confidential paper documents/documents containing personal information should be kept in a secure area.

14.0 SUBJECT ACCESS REQUIEST UNDER GDPR

14.1 An individual has the right to obtain confirmation as to whether personal data concerning them is being processed.

14.2 **How to Make a Subject Access Request:** You can make a request in writing to the Data Protection Officer (DPO), or you can submit an access request electronically. Where a request is received by electronic means, the Services will provide the requested information in an electronic form *(unless otherwise requested by the data subject).*

Subject Access Requests should be addressed to:

Ms. Mary McGrath,
Data Protection Officer,
Carriglea Cáirde Services,
Carriglea,
Dungarvan,
Co. Waterford. Eircode: X35 Y950

14.3 **When Carriglea Cáirde Services receives an Access Request the following is the process:**

a. **Identity Verification:** Subject Access Requests (SAR) are passed to the DPO as soon as received and the request is recorded. The DPO uses all reasonable measures to verify the identity of the individual making the access request, especially where the request is made using online services.

If a third party, relative or representative is requesting information on your behalf, the Services will verify their authority to act for you and may contact you to confirm their identity and gain your authorisation prior to actioning the request.

b. **Information Gathering:** If you have provided enough information in your SAR to collate the personal information held about you, the Services will gather the relevant documents and provide the information in an acceptable format. If the Services do not have enough information to locate your records, we may contact you for further details. This will be done as soon as possible and within the timeframes set out below.

c. **Information Provision:** Once the Services have collated the personal information held about you, we will send it to you in writing (*or in electronic form if requested*). The information will be in an accessible format, using clear and plain language.

14.4 Fees and Timeframes: Whilst the Services provide the information requested without a fee, further copies requested may incur a charge to cover administrative costs.

The Services aims to provide the requested information as soon as possible, but at a maximum, 30 days from the date the request is received. However, where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended by two further months. If this is the case, we will write to you within 30 days and keep you informed of the reason for the delay.

14.5 **Your Right to amendment or erasure of personal data:** Under GDPR, data subjects have the right to request rectification of any inaccurate data held by the Services. Where the Services are notified of inaccurate data, and agree that the data is incorrect, the details will be amended as soon as possible, but within 30 days. You will be informed in writing of the correction and where applicable, provided with the details of any third-party to whom the data has been disclosed.

If the Services are unable to act in response to a request for rectification the reason will be explained in writing.

In certain circumstances, you may also have the right to request the erasure of your personal data or to restrict or object to the processing of your personal data. You can contact the DPO to make such requests.

14.6 **Exemptions and Refusals:** The GDPR contains certain exemptions from the provision of personal information. If an exemption applies to your subject access request, the Services shall inform you as soon as possible, or at the latest, within one month of receipt of the request.

Where possible, the Services will provide you with the reasons for not providing the information and of your right to appeal to the Supervisory Authority.

14.7 **Making a Complaint to the Supervisory Authority;** If you are dissatisfied with the actions of Carriglea Cáirde Services in response to a data request, you have the right to lodge a complaint with the Irish Data Protection Supervisory Authority. The Office of the Data Protection Commissioner can be contacted at:

Office of the Data Protection Commissioner,
Canal House
Station Road
Portarlington
Co. Laois. Eircode: R32 AP23

Telephone	+353 57 8684800 / +353 (0)761 104 800
Lo Call Number	1890 252 231
Fax	+353 57 868 4757
E-mail	info@dataprotection.ie

15.0 DATA PORTABILITY

15.1 The GDPR introduces the right to data portability. This means you can request and receive personal data that you have previously provided in a commonly used and machine-readable format. The right also means you can request one data controller to transfer your personal data to another controller.

Carriglea Cáirde Services provides all personal information pertaining to a data subject to them on request and in a format that is easy to read.

Personal data will be transmitted directly to a designated controller, where technically feasible.

16.0 DATA BREACHES

16.1 The definition of a personal data breach is any incident of security, lack of controls, system or human failure, error or issue that leads to, or results in, the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

16.2 Carriglea Cáirde Services is obliged to report data breaches to the Office of the Data Protection Commissioner in certain circumstances. The Service has controls in place for preventing data breaches and for managing breaches in the event that they do occur. All data breaches will be investigated and a record maintained.

16.3 As soon as a data breach has been identified, it must be reported to the direct line manager and the Data Protection Officer immediately so that breach procedures can be initiated and followed without delay.

16.4 As soon as an incident has been reported, measures must be taken to contain the breach and to stop any further risk/breach prior to investigation and reporting. The measures taken are noted on the *Data Breach Incident Form* in all cases.

16.5 In cases of data breaches, the **Data Protection Officer** is responsible for carrying out a full investigation, recording the outcome/actions on the *Data Breach Incident form* and making any relevant and legal notifications. The outcome of any investigation will be communicated to those involved in the breach.

16.6 Where an incident gives rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data, in manual or electronic form, immediate consideration must be given to informing those affected.

16.7 If the data concerned is protected by technological measures (e.g. encryption) to make it unintelligible to an unauthorised person, there may be no risk to the data and therefore no need to inform data subjects. This would only be justified where the technological measures were of a high standard.

16.8 If applicable, the Office of the Data Commissioner is notified in accordance with the GDPR requirements. The Supervisory Authority protocols are to be followed and their '***Security Breach Notification Form***' should be completed and submitted.

16.9 All incidents of loss of control of personal data in manual or electronic form by a data processor must be reported to the relevant data controller as soon as the data processor becomes aware of the incident.

16.10 The Data Protection Officer will report to the Office of the Data Protection Commissioner in accordance with the Personal Data Security Breach Code of Practice which is available on the web-site of the Office of the Data Protection Commissioner.

16.11 Breach Risk Assessment:

Where the data breach is the result of **human error**, an investigation into the cause will be conducted and a formal interview with the employee(s) may be held.

A review of the procedures associated with the breach is conducted and a risk assessment completed in accordance with the Services Risk Assessment Procedures. Any identified gaps that are found to have caused/contributed to the breach are revised and measures put in place to mitigate any future occurrence of the same root cause.

Where the data breach is the result of a **system error/failure**, the IT will work with the DPO to assess the risk and identify any gaps found to have caused or contributed to the breach. Appropriate actions should be taken to:

a. Attempt to recover any lost equipment or personal information
b. Shut down an IT system if necessary
c. Use back-ups to restore lost, damaged or stolen information
d. Enhance security measures
e. If the incident involves any passwords, these passwords may need be changed immediately.

The DPO will keep a log and report detailing the nature of the incident, steps taken to preserve any evidence, notes of any interviews or statements, the assessment of risk/investigation and any recommendations for future work/actions. This documentation will be retained for a period of 6 years.

5.12 **Breach Notification:**

All incidents where a data breach presents a risk to the affected individuals must be reported to the Office of the Data Protection Commissioner. The only exceptions are when the individuals affected have already been informed and the loss affects no more than 100 data subjects and the loss involves only non-sensitive, non-financial personal data. Such breaches must be reported within 72 hours of the Services becoming aware of the breach

5.13 Data Breaches must be e-mailed to the Office of the Data Protection Commissioner (breaches@dataprotection.ie) using the National Breach Notification Form which is available on their website. Guidance on making a notification is also available on the data protection commissioner's website.

5.14 Where a breach is likely to result in a high risk to the affected individuals, those individuals must be informed without undue delay. The Services reserves the right not to inform the data subject of a personal data breach where the appropriate technical and organisational measures have been implemented which render the data unintelligible to any person who is not authorised to access it *(i.e. encryption, etc.)* or where subsequent measures have been taken which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise.

5.15 Even where it is determine there is no risk to affected individuals following a personal data breach, an internal record of the details has to be kept. The record must state the means for deciding there was no risk, who decided there was no risk and the risk rating that was recorded.

17.0 FREEDOM OF INFORMATION (FOI)

Carriglea Cáirde Services is subject to the terms of the 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:

a. know what information is held in the services records about him/her, subject to certain exemptions to protect key interests;
b. have inaccurate personal material on file corrected;
c. 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 publishes the following information on its web-site:

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

18.0 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:

a. stating that the request is made under the FOI Act
b. setting out sufficient particulars to enable the record to be identified
c. specifying the preferred form of access, if he/she has such a preference (e.g. inspection of the originals, photocopy, etc.).

d. 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.