

## Data Protection Policy

<b>Document reference number/code</b>	Gen 008	<b>Document developed by:</b>	<b>Name and title:</b> Catherine Slattery, <i>Director of Rehabilitation</i> Marianne Coady, <i>Senior Administrator, CEO Office</i> Helen Donovan, <i>ADON Quality &amp; Compliance</i>
		<b>Document reviewed by:</b>	<b>Name and title:</b> <u>Kate Keay</u>
<b>Version No:</b>  1		<b>Recommend for authorisation:</b>	<b>Signature:</b> <u>Helen Donovan</u> <b>Date:</b> <u>8.10.2018</u>
<b>Effective from:</b>  <b>Review Date:</b>	July 2018  July 2021	<b>Authorised by:</b>	<b>Director of service</b> <b>Signature:</b> <u>C. Slattery</u> <b>Date:</b> <u>23/08/18</u>  <b>Chief Executive Officer</b> <b>Signature:</b> <u>S. Colcoran</u> <b>Date:</b> <u>09-10-18</u>
<b>Responsibility for monitoring and audit:</b>		<b>Department Manager</b> Once yearly DP leads	

## Table of Contents

	Page
<b>1.0 Policy statement</b> .....	<b>2</b>
<b>2.0 Purpose</b> .....	<b>2</b>
<b>3.0 Scope</b> .....	<b>2</b>
<b>4.0 Legislation/other related policies</b> .....	<b>2</b>
<b>5.0 Glossary of Terms and Definitions</b> .....	<b>2</b>
<b>6.0 Roles and Responsibilities</b> .....	<b>3</b>
<b>7.0 Policy procedure</b> .....	<b>3- 7</b>
<b>7.1</b> Data Protection Principles	
<b>7.2</b> Data Processing Policy Requirements	
<b>7.3</b> Processing of Special Categories of Personal Data	
<b>7.4</b> Processing of Personal Data	
<b>7.5</b> Data Storage Limitation policy	
<b>7.6</b> Data Anonymisation and Pseudonymisation	
<b>7.7</b> Unauthorised Disclosure	
<b>7.8</b> Third Part Transfer policy	
<b>7.9</b> Third Party Relationships Policy	
<b>7.10</b> Education Policy	
<b>8.0 Revision and Audit</b> .....	<b>7</b>
<b>9.0 References</b> .....	<b>7</b>
<b>10.0 Appendices</b> .....	<b>8-11</b>
<b>Appendix I</b> Glossary of Terms	
<b>Appendix II</b> Acknowledgement sheet	

## 1.0 Policy Statement

The objective of this Data Protection Policy is to set out the requirements of the ORGANISATION relating to the protection of personal data where we act as a Data Controller and / or Data Processor, and the measures we will take to protect the rights of data subjects, in line with EU and Irish legislation.

In the course of our work, we are required to collect and use certain types of information about people (hereafter referred to as data subjects in line with the regulation), including 'personal data' as defined by the General Data Protection Regulation (GDPR). This information can relate to patients, service users, current, past and prospective employees, suppliers and others with whom staff communicate. In addition, staff may occasionally be required to collect and use certain types of personal information to comply with the requirements of other legislation for example infectious diseases legislation and the National Cancer Registry. This document sets out to ensure compliance with the GDPR.

## 2.0 Purpose

Organisation must comply with all applicable data protection, privacy and security laws and regulations (collectively referred to as requirements) in the location in which we operate. Through maintaining a high standard of data protection the Organisation wants to foster a culture that is honest, compassionate, transparent and accountable.

## 3.0 Scope

This policy applies to all organisation staff, students, interns and work experience candidates, contractors, sub-contractors, agency staff and authorised third party commercial service providers and other persons or entities when receiving, handling or processing personal data as defined by the GDPR.

This policy applies to all forms of data including computer, manual and CCTV records relating to citizens.

## 4.0 Legislation/other related policies

### EU Legislation

ECD Guidelines on Data Protection (1980).

EU Communication Regulations (2011).

### Irish Legislation

Irish Constitution 1937 Article 40.3.

Data Protection Act (1988).

Data Protection (Amendment) Act (2003).

Electronic Communications Regulations (2011).

General Data Protection Regulation (2018).

### Peamount Policy

Human Rights Policy incorporating the Rights Review Committee.

Confidentiality Policy.

## 5.0 Terms and Definitions

A list of terms used throughout this policy is defined in Appendix A.

## 6.0 Roles and Responsibilities

### 6.1 GDPR Leads

The GDPR leads are required to be involved in a timely manner, in all issues which relate to the protection of personal data.

They are responsible for monitoring compliance with the GDPR and have overall control of how data is processed within the organisation.

This will include:

- Collecting information about processing activities.
- Analysing and checking the compliance of processing activities.
- Informing, advising and issuing recommendations management and the relevant data processors and controllers.
- Where a national unified or coordinated response is needed, co-operation/collaboration with other organisations DPOs may take place.

### 6.2 Enforcement

The organisation reserves the right to take such action as it deems appropriate against individuals who breach the conditions of this policy. Organisational staff that breach this policy may be subject to disciplinary action as provided for in the organisations disciplinary procedure. If a breach occurs due to reckless behaviour and is knowingly not reported, the person responsible may be held accountable.

Where a breach of this policy is committed by contractors, sub-contractors, agency staff and authorised third party commercial service providers, the organisation reserves the right to remedy via the contracts in existence.

## 7.0 Policy/procedure

It is the policy of the organisation that all data is processed and controlled in line with the principles of the GDPR and relevant Irish legislation.

### 7.1 Data Protection Principles

The following data protection requirements apply to all instances where personal data is stored, transmitted, processed or otherwise handled.

The organisation will comply with the following high level principles:

- Personal data shall only be processed fairly, lawfully and in a transparent manner (Principles of Lawfulness, Fairness and Transparency).
- Personal data shall be obtained only for specified, explicit, lawful, and legitimate purposes, and shall not be further processed in any manner incompatible with those purposes (Principle of Purpose Limitation).

- Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (Principle of Data Minimisation).
- Personal data shall be accurate, and where necessary kept up to date (Principle of Accuracy).
- Personal data shall not be kept for longer than is necessary for the purposes for which the personal data are processed (Principle of Data Storage Limitation); Personal data will be retained in line with the organisation data retention policies.
- Personal data shall be processed in a secure manner, which includes having appropriate technical and organisational measures in place to:
  - (1) prevent and / or identify unauthorised or unlawful access to, or processing of, personal data; and
  - (2) prevent accidental loss or destruction of, or damage to, personal data (Principles of Integrity and Confidentiality).

The organisation shall be responsible for, and be able to demonstrate compliance with, these key principles. (Principle of Accountability).

In addition, the organisation will ensure that data subject's rights are protected as set out in the GDPR.

- Data subjects will be able to request access to data we hold on them through a Subject Access Request (SAR) (Right of Access).
- Data subjects can request to change or correct any inaccurate data (Right to Rectification).
- Data subjects have the right to object to having their data processed (Right to Restriction of Processing).
- Data subjects can request to delete data that we hold excluding medical Records (Right to Erasure (sometimes referred to as the Right to be Forgotten)).
- Data subjects can request to have their data moved outside of the organisation if it is in an electronic format (Right to Data Portability).
- Data subjects can object to a decision made by automated processing, with certain limited exceptions (such as legitimate grounds for the processing or the defence of legal claims) and request that any decision made by automated processes have some human element (Right to Object to Automated Decision Making, including Profiling).

## 7.2 Data Processing Policy Requirements

The organisation, as a Data Controller, shall be responsible for, and be able to demonstrate compliance with these GDPR Requirements.

- We will process personal data in accordance with the rights of data subjects.
- We will communicate with data subjects in a concise, transparent, intelligible and easily accessible form, using clear language.
- We will only transfer personal data to Third Parties within Ireland and outside of the We European Economic Area (EEA) in accordance with this policy.
- We shall conduct all personal data processing in accordance with legitimate GDPR based processing conditions in particular;
  - Data subject consent for one or more specific purposes not covered under the



processing of special categories of personal data.

Or

- Necessary processing for contract performance or contract entry.

Or

- Legal obligation underpinning processing.

### 7.3 Processing of Special Categories of Personal Data

Special categories of data are defined by the GDPR and include data such as racial or ethnic origin, religious or philosophical beliefs, genetic data, biometric data, health data, sex life details and sexual orientation.

The processing of special categories of personal data shall be lawful where it is necessary—

- (a) for the purposes of preventative or occupational medicine.
- (b) for the assessment of the working capacity of an employee.
- (c) for medical diagnosis.
- (d) for the provision of medical care, treatment or social care.
- (e) for the management of health or social care systems and services.

or

(f) pursuant to a contract with a health professional.

Processing is lawful where it is undertaken by or under the responsibility of—

- (a) a health practitioner, or
- (b) a person who in the circumstances owes a duty of confidentiality to the data subject that is equivalent to that which would exist if that person were a health practitioner. For example the Outpatient Clinic Secretary, Emergency Department Receptionist, Primary Care Centre Staff etc.

If the processing of data is not covered by the categories above the organisation will require explicit consent from the data subject.

### 7.4 Processing of Personal Data

- 7.4.1** The processing is necessary in order to protect the vital interests of the person (referred to as the data subject in Data Protection language). This would apply in emergency situations such as in the Emergency Department when unconscious sharing information with other emergency services for rescue or relocation during severe weather events etc.
- 7.4.2** The processing is necessary for a task carried out in the public interest or in the Exercise of official authority vested in the controller; for the organisation this official Authority is vested in us through the Health Act 2004 (as amended).
- 7.4.3** Processing of personal data is permitted where is necessary for the Performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

### 7.5 Data Storage Limitation Policy

The organisation should erase any personal data that violates;

- Data Protection Law
- Data Protection Regulations

- Contractual Obligations
- Requirements of this Policy
- If the organisation no longer requires the Data

### 7.6 Data Anonymisation and Pseudonymisation

The organisation must anonymise and/ or pseudonymise personal data when it is being used for purposes other than the direct provision of public health and health and social care services.

### 7.7 Unauthorised Disclosure

All persons covered under this policy are prohibited from disclosing a data subject's confidential information (including personal data or special categories of personal data), unless this policy or a legal basis allows for such disclosures.

All persons covered under this policy must report all suspected incidents of unauthorised access to the relevant GDPR Lead. Incidents include disclosure, loss, destruction or alteration of patient and service user's personal information, regardless of whether it is in paper or electronic form.

The organisation has established formal procedures for reporting suspected incidents of unauthorised disclosure of data/data breach.

The organisation aims to use its systems and processes which are guided by strict adherence to data protection legislation in the delivery of health and social care services.

If any staff member considers that particular class of personal data processing may affect a data subject's rights and freedoms then they should engage the GDPR Lead.

### 7.8 Third Party Transfer Policy

The organisation must not transfer personal data to a Third Party outside of the EEA regardless of whether the organisation is acting as a Data Controller or Data Processor unless:

**7.8.1** The EU recognises the transfer country/territory as having an adequate level of data subject legal protection relating to personal data processing or

**7.8.2** The EU recognises the transfer mechanism as providing adequate protection when made to countries/territories lacking adequate legal protection. Please see <https://www.dataprotection.ie/docs/Transfers-Abroad/1244.htm>

**7.8.3** The explicit consent of the data subject is required to allow Third Party transfer or transfer is authorised by law.

**7.8.4** All reasonable, appropriate and necessary steps have been taken to maintain the required level of Personal Data Protection; and Subject to the provisions above, including any necessary organisational approvals, the organisation may transfer personal data to a Third Party outside of the EEA where any of the following apply:

**7.8.5** The transfer is necessary to protect the data subject's vital interests; or

**7.8.6** The data subject has given explicit consent to the proposed transfer;

Or

**7.8.7** The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the organisation and a Third Party;

Or

- 7.8.8** The transfer is necessary or legally required for the establishment, exercise, or defence of legal claims; or
- 7.8.9** The transfer is required by law; or
- 7.8.10** The transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest. The DPO must assess whether any of the above exceptions apply prior to any personal data transfer and must record the determination in writing.

### **7.9 Third Parties Relationships Policy**

Where the organisation engages a Third Party for processing activities, this Data Processor must protect personal data through sufficient technical and organisational security measures and take all reasonable GDPR compliance steps.

When engaging a Third Party for personal data processing, the organisation must enter into a written contract, or equivalent. This contract or equivalent shall:

- 7.9.1** Clearly set out respective parties responsibilities.
- 7.9.2** Must ensure compliance with relevant European and local Member State Data Protection requirements/legislation.
- 7.9.3** At the expiry of a data processor contract the data processor is contractually obliged To return the full dataset to the ORGANISATION and provide unequivocal evidence that their copy of the dataset is erased.

The organisation must ensure that all Third Party relationships are established and maintained. Data processors who are processing data on behalf of the organisation must secure approval from the organisation if they wish to engage further data processors.

### **7.10 Education and Awareness Policy**

The organisation will ensure that General Data Protection Regulation training material is available to all staff.

## **8.0 Revision and Audit**

This policy will be reviewed and updated every 3 years or more frequently if necessary to ensure any changes to the organisation's structure and business practices are properly reflected in the policy.

## **9.0 References**

N/A



## Appendix I Glossary of Terms

Term	Description
<b>Anonymised</b>	Means the process of making personal data anonymous data. 'Anonymise' should be construed accordingly.
<b>Anonymous Data</b>	Means any information relating to a natural person where the person cannot be identified, whether by the Data Controller or by any other person, taking account of all the means reasonably likely to be used either by the Data Controller or by any other person to identify that individual.
<b>Biometric Data</b>	Means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images
<b>Consent</b>	Means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
<b>Data</b>	<p>As used in this Policy shall mean information which either:</p> <ul style="list-style-type: none"> <li>- is processed by means of equipment operating automatically in response to instructions given for that purpose;</li> <li>- is recorded with the intention that it should be processed by means of such equipment;</li> <li>- is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system;</li> <li>- Does not fall within any of the above, but forms part of a readily accessible record.</li> </ul> <p>Data therefore includes any digital data transferred by computer or automated equipment, and any manual information which is</p>
<b>Data Controller</b>	Means a person or organisation who (alone or with others) determines the purposes for which and the manner in which any personal data are, or are to be, processed. A Data Controller can be the sole Data Controller or a joint Data Controller with another person or organisation.
<b>Data Processor</b>	Means a person or organisation that holds or processes personal data on the instructions of the Data Controller, but does not exercise responsibility for, or control over the personal data.
<b>Data Protection</b>	Means the protection of personal data
<b>Data Protection Commissioner</b>	Means the office of the Data Protection Commissioner in Ireland.
<b>Data subject</b>	Refers to the individual to whom personal data held relates, including: employees, customers, suppliers.
<b>DPO</b>	Data Protection Officer

<b>EEA</b>	<p>European Economic Area</p> <p>Means the area in which the Agreement on the EEA provides for the free movement of persons, goods, services and capital within the European Single Market, as well as the freedom to choose residence in any country within this area.</p>
<b>Encryption</b>	<p>It is the process of encoding information stored on a device and can add a further useful layer of security. It is considered an essential security measure where personal data is stored on a portable device or transmitted over a public network.</p>
<b>EU Directive</b>	<p>Means the EU Data Protection Directive 95/46/EC.</p>
<b>Genetic Data</b>	<p>Means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question</p>
<b>Health Practitioner</b>	<p>Means a registered medical practitioner within the meaning of section 2 of the Medical Practitioners Act 2007 or a medical practitioner practising medicine pursuant to section 50 of that Act, a registered dentist within the meaning of section 2 of the Dentists Act 1985,</p> <p>a registered pharmacist or registered pharmaceutical assistant within the meaning of the Pharmacy Act 2007, a registered nurse or registered midwife within the meaning of section 2(1) of the Nurses and Midwives Act 2011, a registered optometrist or registered dispensing optician within the meaning of section 2 of the Opticians Act 1956, a registrant within the meaning of section 3(1) of the Health and Social Care Professionals Act 2005, a person whose name is entered in the register of pre-hospital emergency care practitioners established under the Pre-Hospital Emergency Care Council (Establishment) Order 2000 (S.I. No. 109 of 2000), or a person who falls within a class of persons, being a</p>
<b>Information Request</b>	<p>Means a request from a data subject relating to that individual's</p>
<b>Personal Data</b>	<p>Means any information relating to an identified or identifiable natural person (Data subject). 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 by reference to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural</p>

<b>Processing</b>	<p>Means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.</p> <p>The terms 'Process' and 'Processed' should be construed accordingly.</p>
<b>Pseudonymisation</b>	<p>Means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable</p>
<b>Personal Data Breach</b>	<p>Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed</p>
<b>Restriction of Processing</b>	<p>Means the marking of stored personal data with the aim of limiting their processing in the future.</p>
<b>SMT</b>	<p>Means the Senior Management Team/Board of the organisation.</p>
<b>Subject Access Request</b>	<p>Means a written request made to a Data Controller by any individual about whom a Data Controller keeps personal data on computer or in a relevant filing system. Response must be provided to the data subject under the terms outlined by GDPR</p>
<b>Third Party</b>	<p>Means an entity, whether or not affiliated with the organisation, that is in a contractual arrangement with the organisation. These Third Party relationships include, but are not limited to, activities that involve outsourced products and services, use of independent consultants, networking and marketing arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, joint ventures and other business arrangements where the organisation has an ongoing relationship. Third Party relationships, for the purposes of this policy, generally do not include customer relationships.</p> <p>Under GDPR a 'Third Party' means a natural or legal person, public authority, agency or body, other than the data subject, controller, processor and persons who, under the direct authority of the Data Controller of Data Processor, are authorised to process personal data.</p>

