Policy / Procedure Details	Title:	**Data Protection Policy**		
	Type:	**Essential Procedure**		
	Related Quality Measure:	**Use of Information**		
	Code:	**1.21B**		
Original Version Details	Date Released:	**22 / 08 / 2019**		
Previous Version(s) Details	Date(s) Released:	**26 / 08/ 2019**	**20/01/2020**	
Current Version Details	Written By:	**Data Protection Officer**		
	Reviewed By:	**Procedural Review Committee**		
	Approved By:	**WCA Board of Directors**		
	Date Released:	**20/01/2023**		
	Monitoring Process:	**Procedural Review Process**		
	Date Due for Review:	**20/01/2026**		

Table of Contents

1. Introduction

Western Care Association needs to collect personal information to effectively carry out our everyday business functions and activities and to provide the products and services defined by our business type. Such data is collected from employees, customers, suppliers and persons we support and includes (but is not limited to), name, address, email address, data of birth, IP address, identification numbers, private and confidential information, sensitive information and bank details.

In addition, we may be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations, however we are committed to processing all personal information in accordance with the General Data Protection Regulation (GDPR), Irish Data Protection laws and any other relevant the Data Protection laws and codes of conduct (herein collectively referred to as "**the Data Protection laws**").

The Organisation has developed policies, procedures, controls and measures to ensure maximum and continued compliance with the data protection laws and principles, including staff training, procedure documents, audit measures and assessments. Ensuring and maintaining the security and confidentiality of personal and/or special category data is one of our top priorities and we are proud to operate a 'Privacy by Design' approach, assessing changes and their impact from the start and designing systems and processes to protect personal information at the core of our business.

Purpose

The purpose of this policy is to ensure that the Organisation 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.

The Data Protection laws include provisions that promote accountability and governance and as such the Organisation has put comprehensive and effective governance measures into 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. This policy also serves as a reference document for employees and third-parties on the responsibilities of handling and accessing personal data and data subject requests.

In the course of our work, we are required to collect and use certain types of information about individuals (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 persons we support, current, past and prospective employees, volunteers, board members, suppliers and other third parties with whom staff communicate. This policy sets out to ensure compliance with the GDPR.

Scope

This policy applies to all Western Care Association staff, persons we support, volunteers, board members, contractors, and all other third parties engaged with the Organisation. It relates to all data including electronic, manual and CCTV records.

Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

Confidentiality
Confidentiality requires that at all times records are maintained securely and that information is safeguarded so that only people who need to access this information can do so. The sharing of information is done on the basis of respect and in order to provide Informed Support. This refers to the need for people who support the person/family to have access to information necessary to fulfil their role properly.

Access
Access means that in the first instance information recorded is routinely shared with the person/ family or that they are aware of and can obtain any record about them which they wish to see unless in the rare cases where there are conflicting legal obligations on the Association. It means ensuring records are written in such a way as to be easily understood and unnecessary technical language is avoided. Access also means that support is provided for the interpretation of records so that the contents are understood. Good practice means that records will be developed in preferred formats that are accessible for the individual.

Consent
Consent means that the family/person is fully informed about the type and the content of records which are kept by the Association through the Privacy Notice. A copy of the current privacy notice is accessible on our website.

Definition
Personal information is considered to be information which would ordinarily be known only to individuals or their family and friends, and/or information relating to the individual that is held by a public body on the understanding that it would be treated as confidential.
Data Protection is the safeguarding of the privacy rights of individuals in relation to the processing of their personal information. According to the Freedom of Information Act, records refer to all information held both in electronic format and in a manual or paper based form and can include; *"any memorandum, book, emails, diaries, plan, map, loose papers, post it notes, drawings, diagram, files, pictorial or graphic work or other document, any photograph, film, tapes, videos, CDs or recording (whether of sound or images or both), any form in which data (within the meaning of the Data Protection Act, 1988) is held, any other form (including machine-readable form) or anything in which information is held or stored manually, mechanically or electronically and anything that is a part or a copy, in any form"*.

A list of terms used throughout the policy are defined in Appendix E

2. The Legal and Policy Context

Data Protection

Data Protection is the safeguarding of the privacy rights of individuals in relation to the processing of personal data. Personal Data means information relating to a living individual who is or can be identified from the data that is in the possession of a Data Controller. The following data protection requirements apply to all instances where personal data is stored, transmitted, processed or otherwise handled regardless of geographic location.

General Data Protection Regulation

The General Data Protection Regulation (GDPR) (EU)2016/679) was approved by the European Commission in April 2016 and apply to all EU Member States from 25th May 2018. As a 'Regulation' rather than a 'Directive', its rules apply directly to Member States, replacing their existing local data protection laws and repealing and replacing Directive 95/46EC and its Member State implementing legislation.

As the Organisation processes personal information regarding individuals (data subjects), we are obligated under the General Data Protection Regulation (GDPR) to protect such information, and to obtain, use, process, store and destroy it, only in compliance with its rules and principles.

Principles of GDPR

Western Care Association will comply with the following principles:

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; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ***('purpose limitation')***
- ***c)*** adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ***('data minimization')***
- ***d)*** accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ***('accuracy')***
- ***e)*** kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ***('storage limitation')***
- ***f)*** processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ***('integrity and confidentiality').***

In addition, Western Care Association shall be responsible for, and be able to demonstrate, compliance with these principles' (accountability)

Processing of Special Categories of Personal Data

Special categories of data are defined by 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.

Conditions for processing of special categories of personal data

a) Explicit consent
b) Necessary for legal claims or judicial purposes
c) Necessary for employment, social security and social protection law
d) Vital interests
e) Legitimate activities with a political, philosophical, religious or trade union aim
f) Where the data subject has already manifestly made the data public
g) Where the processing of special category personal data is necessary for reasons of substantial public interest, on the basis of EU or Member State law.
   The data processing must be:
   - proportionate to the aim pursued
   - respect the essence of the right to data protection and
   - provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
h) Provision of health care
i) Archiving purposes in the public interest
j) Public interest in the area of public health

Privacy Notices

Western Care Association has a responsibility to demonstrate compliance with the requirements of GDPR. Being transparent and providing information to individuals about how we use their personal data is a key requirement of the General Data Protection Regulation.

We are required to provide each Data Subject, by way of a **Privacy Notice**, outlining all the necessary and legal information about how, why and when we process their data, along with their rights and obligations. The following are the notices we have in place;

You can access these Privacy Notices on our website on www.westerncare.com

Your Rights

Under the GDPR, you have the right to request rectification of any inaccurate data held by us.

Where we are notified of inaccurate data, and agree that the data is incorrect, we will amend the details immediately as directed by you and make a note on the system (or record) of the change and reason(s).

We will rectify any errors within 30 days and inform you in writing of the correction and where applicable, provide the details of any third-party to whom the data has been disclosed.

If for any reason, we are unable to act in response to a request for rectification and/or data completion, we will always provide a written explanation to you and inform you of your right to complain to the Supervisory Authority and to seek a judicial remedy.

In certain circumstances, you may also have the right to request from the Organisation, the erasure of personal data or to restrict the processing of personal data where it concerns your personal information; as well as the right to object to such processing. You can use the Data Protection Officer to make such requests. The organisation must fulfil to your request immediately unless the processing of your data is required to comply with our legal obligations and, where necessary, to protect our legitimate business interests

Responsibilities for Staff around Data Protection

- **Obtain and process information fairly** - seek consent, where appropriate; inform persons we support/families about the type of information we hold and why it is required (this is communicated through our Privacy Notices)
- **Keep data for one or more specified, explicit and lawful** purposes - be aware of what purpose you are keeping information for.
- **Use and disclose information only for such purposes** - would a person we suport/family member be surprised to learn that a particular use of or disclosure of their information is taking place? Ensure that this would not be the case.
- **Users are prohibited from disclosing a data subjects personal information to a third party**, unless there is a legal basis which allows for such disclosures
- **Kept information safe and secure** - "password protect" computer systems; dispose of records carefully; secure premises when unoccupied; access to personal information on a need to know basis.
- **Kept it accurate**; complete and up-to date - yearly audit of database; records maintained in an orderly manner;
- **Ensure that it is adequate, relevant and not excessive** - do you keep only the minimum amount of personal information which you need to keep to carry out your job in accordance with the procedures of the organization?
- **Retain it no longer than is necessary for the purpose** - Retention policy in operation which ensures that records are kept for a specified period;
- **Give individuals /families a copy of their personal information, on request**. These requests must be directed to the Data Protection Officer who will arrange for records to be made available following review.

3. Informing Person we support /Families, Volunteers and Staff about Records

We are required to provide each Data Subject, by way of a **Privacy Notice**, outlining all the necessary and legal information about how, why and when we process their data, along with their rights and obligations. This will inform them about who requires access to the information held, and the purpose for the access and how they can access their information.

The following are the notices we currently have in place:

- Privacy Notice for **Individuals using Western Care Association Services**
- Privacy Notice for **Employees** of Western Care Association

- Privacy Notice for **Members of the Board of Directors**
- Privacy Notice for **Volunteers volunteering with Western Care Association**

On admission to the Services, the person/family will be provided with a Privacy Notice. Each service will determine who best to do this but it is generally undertaken by the Social Worker or a manager.

Other Information Purposes
Anyone outside of the Person's main service supports must ask the person/family's permission before they access their information this should be done in writing, and must be done according to the wishes of the person/family. Staff must also seek consent from the individual involved prior to displaying photos/information in any public area. The Association will not release any information without appropriate consent. The organisation should provide only the information that is relevant. Consents should be limited to certain pieces of information, for a particular purpose, and be in effect for a specified period of time.
Please contact the Data Protection Officer before releasing any information to third parties.

4. Access to Records

All persons covered under this policy are prohibited from disclosing personal information, unless there is a legal basis allows for such disclosures. All efforts should be made to ensure that personal information is protected and only be shared when necessary.

Access means that in the first instance information recorded is routinely shared with the person/ family or that they are aware of and can obtain any record about them which they wish to see unless in the rare cases where there are conflicting legal obligations on the Association. It means ensuring records are written in such a way as to be easily understood and unnecessary technical language is avoided. Access also means that support is provided for the interpretation of records so that the contents are understood. Good practice means that records will be developed in preferred formats that are accessible for the individual.

Requests for access to records should be directed through the Data Protection Officer. The DPO will be able to advise you on the best direction to take to access your information i.e. Data Subject Access Request or an FOI Request (see FOI Policy)

The Right of Access
Individuals (Data Subjects) can request access to data we hold on them through a Subject Access Request (SAR) or an FOI Request. Data needs to be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Such information is provided free of charge and is in writing, or by other means where authorised by the data subject and with prior verification as to the subject's identity (i.e. verbally, electronic).

Data Subject Access Request (SAR)
GDPR gives individuals the right to know what information is held about them, to access this information and to exercise other rights, including the rectification of inaccurate data.

The GDPR is a regulatory framework which ensures that personal information is obtained, handled and disposed of properly.

How to make a Subject Access Request?
You can make a SAR in writing using the form attached (Appendix B – RMD 5), or by emailing the Data Protection Officer (DPO). You may need to provide a form of identification as part of the request.

Subject Access Requests (SAR) are passed to the DPO as soon as they are received. We will utilise the request information to ensure that we can verify your identity and where we are unable to do so, we may contact you.

If you have provided enough information in your SAR to collate the personal information held about you, we will gather all documents relating to you and ensure that the information required is provided in an acceptable format. If we do not have enough information to locate your records, we may contact you for further details.

If a third party, relative or representative is requesting the information on your behalf, we will verify their authority to act for you and again, may contact you to confirm their identity and gain your authorisation prior processing the request.
The Organisation always aims to provide the requested information at the earliest convenience, 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 delay and provide the reasons.

Procedure for Staff - Routine Access to Records
Western Care Association supports the right of an individual to see what information is held about him or her within the organisation as defined in the Data Protection Act. Staff should contact their Line Manager if they wish to view their file. All requests will be examined by the Data Protection Officer. Where routine viewing access cannot be granted, the requester should be made aware that his/her request could be made under Freedom of Information or Subject Access Request.

Procedure for Services Users and Families - Routine Access to Records
The primary principle of our Records management practice is that the person/family has access to their information in the first instance by right. Western Care Association supports the right of an individual and the family of a minor to see what information is held about him or her within the organisation as defined under Data Protection. As a matter of policy and good practice and in line with legislation, all information about a person or family should be shared with them in the first instance unless there is a clear reason not to do so. Where routine viewing access cannot be granted, the requester should be made aware that his/her request could be made under Freedom of Information or Subject Access Request.

Process around Routine Access to Records

- All requests are made in writing (through completion of form Appendix A (RMD 1) and addressed to the Data Protection Officer
- Requester should state what records are being sought
- The completed form should be accompanied by appropriate identification (in cases where the requester is not known to the organisation)

All requests made through this route will automatically be examined under Data Protection Act and if it emerges that sensitive information or exempted information is contained in the files, the person/family will be advised and supported to apply through the Freedom of Information route.

In releasing information Western Care Association will always have regard to the individual's privacy, confidentiality and the public interest.

Exemptions to Routine Access Process

There are a number of exceptions to routine access and particular care should be taken when dealing with records that contain sensitive information. Listed below are examples where FOI Access would be the appropriate route to take:

- Documents relating to a suspected or actual child abuse case
- Documents revealing the involvement and deliberations of an investigation into alleged sexual abuse
- Documents containing information in relation to testing for and/or treatment of HIV/AIDS (including statements regarding HIV Status) or other notifiable diseases under the Health Acts
- A deceased person's health records
- In circumstances where it is considered that the health record contains matter about a third party or information received in confidence from a third party
- Any other sensitive matter such as documents revealing confidential sources of information

The requester should be informed that such requests should be made through the Freedom of Information Act and the requester should be forwarded to the FOI Officer.

Exemptions to Routine Access Process

There are a number of exceptions to routine access and particular care should be taken when dealing with records that contain sensitive information. Listed below are examples where FOI Access would be the appropriate route to take:

- Documents relating to a suspected or actual child abuse case
- Documents revealing the involvement and deliberations of an investigation into alleged sexual abuse
- Documents containing information in relation to testing for and/or treatment of HIV/AIDS (including statements regarding HIV Status) or other notifiable diseases under the Health Acts
- A deceased person's health records
- In circumstances where it is considered that the health record contains matter about a third party or information received in confidence from a third party

- Any other sensitive matter such as documents revealing confidential sources of information

The requester should be informed that such requests should be made through the Freedom of Information Act and the requester should be forwarded to the FOI Officer.

Fees and Timeframes

Western Care Association aims to complete all access requests within 30 days of receipt of the request and verification and provide the information free of charge. Where the request is made by electronic means, the information will be provided in electronic format, unless an alternative format is requested.

While the information requested is provided without a fee, further additional copies requested by the individual a charge may be applied to cover administrative costs. This situation could arise where the request is considered to be voluminous incurring significant time to process the request. The Data Protection Officer will advise you of this decision and will support you to refine your request should you wish to do so.

Access for purposes of Research, Training or Evaluation
Access to information held on files may be granted to staff of Western Care Association who are involved in particular research, training or evaluation projects which have been authorised by the Chief Executive Officer on advice from the Management Team subject to:

- Individuals and/or Families being provided with a written explanation of the purposes of the research/training,
- Specifying the precise information they wish to access,
- Specifying the ways in which the information obtained will be used, and
- Obtaining written consent from Individuals and/or Families.

Access by professionals who are not employees of Western Care Association
Professionals who are not employees of Western Care Association will not have access to services users' files.

When a person we support is transferring to another agency, all relevant information will be provided if requested with the written permission of the person we support /parent guardian.

These requests should be directed through the Data Protection Officer.

Procedure for Access by External Sources - Release of records to External Agencies (i.e. Schools, HSE Therapists. CAMH's, GMIT, etc.)

In the case of any external agency requesting a copy of a report/record, consent must always be sought in writing from the person we support and/or family, where appropriate, prior to release.

Care should be taken to establish the identity of the recipient of the information, the recipient's name and authority to receive the information should be checked prior to the release of the information. Where the parents no longer reside together, consent should be sought from both individuals separately. Exceptions to this would be where one of the parents cannot be contacted. The Consent letter should be placed on the electronic folder of the person we support it relates to.

These requests should be directed through the Data Protection Officer.

Release of records to a solicitor

In litigation involving Western Care, where an Order for Discovery is sought by letter, the Associations' Insurer's solicitors ordinarily deal with the matter. A request will be made through the Associations' Insurer's solicitors seeking access to specified records in their possession. The solicitor will prepare an Affidavit seeking out full details of all documents and other records held by Western Care which are relevant to the case. Prior to the release of any records the following information should be sought from the Associations' Insurer's solicitors:

- The request should be in writing
- The solicitor's letter should outline what records are being sought and for what calendar period
- The deadline for receipt of the records by the solicitor
- The records requested will be copied and either sent by registered post or collected by the solicitor

Other Mechanisms for Access

Requests could also come from other sources such as Order of Discovery; Garda Investigations, Post Mortems, Court Subpoena, Search Warrant, Court Orders, Request/Investigation of Information Commissioner or Ombudsman or an Officer authorised by the Minister for Health and Children. These will be evaluated individually and handled through the appropriate request process.

5. Data Security and Breach Requirements

This applies to all employees, service providers and third parties that access, use, store or process information on behalf of Western Care Association

The Organisation's 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, regardless of whether it is in paper or electronic form.

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.

Breach Management Plan
The Data Protection Officer is responsible for the review and investigation of any data breach involving personal data, regardless of severity, impact or containment. All data breaches will be investigated, even where notifications and reporting are not required, and we retain a full record of all data breaches to ensure gap and analysis are available and used.

Breach Notification
As soon as a data breach has been identified, you must report the breach to your manager and the Data Protection Officer immediately. Reporting incidents in full and with immediate effect is essential to the compliant functioning of the organisation and is not about apportioning blame.

As soon as an incident has been reported, measures must be taken to contain the breach. The aim of any such measures should be to stop any further risk/breach to the organisation, prior to investigation and reporting.

Western Care Association applies a Breach Incident Form for all incidents, which is completed for any data breach, regardless of severity or outcome. This will be completed by the DPO with the support of the person who was involved in the breach and the person who identified the breach. This will help gather the necessary information in the cases where the Supervisory Authority needs to be notified.

In cases of data breaches, the **Data Protection Officer** is responsible for carrying out a full investigation, appointing the relevant staff to contain the breach, gathering details of the incident on and making any relevant notifications.

A full investigation is conducted and recorded on the incident form, with the outcome being communicated to all staff involved in the breach, in addition to senior management. A copy of the completed incident form is filed for audit and documentation purposes.

If applicable, the Supervisory Authority must be notified within 72 hours. The Authority has a specific Online Breach Reporting Form on their website which the DPO will complete and submit which provides detailed information on the data breach.

Data Subject Notification
When a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, we will always communicate the personal data breach to the data subject without undue delay, in a written, clear and legible format. This is in accordance with the GDPR requirements.

The notification to the Data Subject shall include: -

- The nature of the personal data breach
- The name and contact details of our Data Protection Officer and/or any other relevant point of contact (*for obtaining further information)*
- A description of the likely consequences of the personal data breach
- A description of the measures taken or proposed to be taken to address the personal data breach *(including measures to mitigate its possible adverse effects)*

We reserve the right not to inform the data subject of any personal data breach where we have implemented the appropriate technical and organisational measures which render the data unintelligible to any person who is not authorised to access it *(i.e. encryption, etc.*) or where we have taken subsequent measures which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise.

A record of all breaches is kept for audit and documentation purposes.

Breach Risk Assessment

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

System Error
Where the data breach is the result of a system error/failure, the IT team are to work in conjunction with the Data Protection Officer to assess the risk and investigate the root cause of the breach. A gap analysis will be completed on the system/s involved and a full review and report to be added to the Breach Incident Form.

Any identified gaps that are found to have caused/contributed to the breach are to be revised and risk assessed to mitigate and prevent any future occurrence of the same root cause.

Assessment of Risk and Investigation
The Data Protection Officer should ascertain what information was involved in the data breach and what subsequent steps are required to remedy the situation and mitigate any further breaches.

The lead investigator should look at: -

- The type of information involved
- It's sensitivity or personal content
- What protections are in place (e.*g. encryption*)?
- What happened to the information/Where is it now?
- Whether there are any wider consequences/implications to the incident

The appointed lead should keep an ongoing log and clear 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.

Supervisory Authority Notification
The Supervisory Authority is to be notified of any breach where it is likely to result in a risk to the rights and freedoms of individuals. These are situations which if the breach was ignored, would lead to significant detrimental effects on the individual.

Where applicable, the Supervisory Authority is notified by the DPO of the breach no later than 72 hours after becoming aware of it by using their Online Reporting Form.

If for any reason it is not possible to notify the Supervisory Authority of the breach within 72 hours, the notification will be made as soon as is feasible, accompanied by reasons for any delay. Where a breach is assessed by the DPO and deemed to be ***unlikely*** to result in a risk to the rights and freedoms of natural persons, we reserve the right not to inform the Supervisory Authority in accordance with Article 33 of the GDPR.

Breach incident procedures are always followed and an investigation carried out, regardless of our notification obligations and outcomes, with reports being retained and made available to the Supervisory Authority if requested.

Where the Organisation acts in the capacity of a controller using an external processor, we have a written agreement in place to state that the processor is obligated to notify us without delay after becoming aware of a personal data breach.

Recording keeping during a data breach
All records and notes taking during the identification, assessment and investigation of the data breach are recorded and authorised by the **Data Protection Officer** and are retained for a period of 6 years from the date of the incident.

6. Data Protection Impact Assessments (DPIA)

Individuals have an expectation that their privacy and confidentiality will be upheld and respected whilst their data is being stored and processed by the Organisation. We therefore utilise several measures and tools to reduce risks and breaches for general processing. However, where processing is likely to be high risk or cause significant impact to a data subject, we utilise proportionate methods to map out and assess the impact ahead of time.

Where the Organisation must or are 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 and freedoms of data subjects, we always carry out a Data Protection Impact Assessment (DPIA) *(sometimes referred to as a Privacy Impact Assessment*).

Carrying out DPIAs enables us to identify the most effective way to comply with our data protection obligations and ensure the highest level of data privacy when processing. It is part of our Privacy by Design approach and allows us to assess the impact and risk before carrying out the processing, thus identifying and correcting issues at the source, reducing costs, breaches and risks.

Checklist for a DPIAs

1. Identify the need for a Data Protection Impact Assessment
   Is DPIA required?
2. Complete Project Brief and Plan.
3. Identify the privacy issues and associated risks.
4. Identify proposed risk solutions and mitigating actions.
5. Integrate outcomes into Project Plan.
6. Authorization and Recording to include reporting the results to Senior Management or Supervisory Authority if required.
7. DPO and Project Lead will monitor Project progress and identify any new risks that need to be reflected in the DPIA.

Contact the DPO if you are introducing new systems where personal data may be at risk.

Enforcement

Western Care Association reserves the right to take such action as it deems appropriate against individuals who breach the conditions of this policy. Staff who breach this policy may be subject to disciplinary action as provided for in the disciplinary procedure. If a breach occurs due to reckless behaviour and a breach occurs 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 HSE reserves the right to remedy via the contracts in existence.

Data Protection Commission
21 Fitzwilliam Square South
Dublin 2
D02 RD28
Phone; 01 7650100 / 1800437 737

(RMD 1)

Request for Person we support to view Main File Records

PART A – To be completed by Named Staff/Person we support

Name of Requester: _____

Date of Request: _____

Person/Named Staff Accompanying Requester_____

Name of Service: _____

Contact Number: _____

Any Special Requirements – please specify (i.e. tape recorder/camera)

_____

PART B – To be completed by FOI Officer

Date Received to FOI Officer: _____

Date File Checked by Decision Maker: _____

Date/time of Visit arranged: _____

Did visit take place: Yes ☐ No ☐

If No, new Date & Time arranged for Visit:_____

- **Western Care will try and facilitate all requests within two working weeks, where possible.**

All requests made through this route will automatically be examined under Data Protection Act and if it emerges that sensitive information or exempted information is contained in the files, the person/family will be advised and supported to apply through the Freedom of Information route.

APPENDIX B

(RMD 5) Subject Access Request Form

Under the General Data Protection Regulation, you are entitled as a data subject to obtain from the Organisation, confirmation as to whether we are processing personal data concerning you, as well as to request details about the purposes, categories and disclosure of such data.

You can use this form to request information about, and access to any personal data we hold about you. Details on where to return the completed form can be found at the end of the document.

1. Personal Details:

Data Subject's Name:		**DOB:**	___ / ___ / _____
Mobile No:		**Email:**	
Data Subject's Address:			
Any other information that may help us to locate your personal data:			

2. Specific Details of the Information Requested:

3. Representatives *(only complete if you are acting as the representative for a data subject)*
***[Please Note:** We may still need to contact the data subject where proof of authorisation or identity are required]*

Representative's Name:		**Relationship to Data Subject:**	
Telephone No:		**Email:**	
Representative's Address:			
I confirm that I am the authorised representative of the named data subject:			

Representative's Name: _____ **Signature:** _____

4. Confirmation

Data Subject's Name: _____ [print name]

Signature: _____ **Date:** ____ /____ /_____

5. Completed Forms

For postal requests, please return this form to:
Data Protection Officer
Western Care Association
John Moore Road
Castlebar
Co. Mayo

For email requests, please return this form to: foiofficer@westerncare.com

APPENDIX C

(RMD 7)

DATA BREACH INCIDENT FORM (FOR INTERNAL USE)

DPO/INVESTIGATOR DETAILS:			
NAME:		**POSITION:**	
DATE:		**TIME:**	
TEL:		**EMAIL:**	
INCIDENT INFORMATION:			
DATE/TIME OR PERIOD OF BREACH:			
DESCRIPTION & NATURE OF BREACH:			
TYPE OF BREACH:			
CATEGORIES OF DATA SUBJECTS AFFECTED:			
CATEGORIES OF PERSONAL DATA RECORDS CONCERNED:			
NO. OF DATA SUBJECTS AFFECTED:		**NO. OF RECORDS INVOLVED:**	
IMMEDIATE ACTION TAKEN TO CONTAIN/MITIGATE BREACH:			
STAFF INVOLVED IN BREACH:			
PROCEDURES INVOLVED IN BREACH:			
THIRD PARTIES INVOLVED IN BREACH:			
BREACH NOTIFICATIONS:			
WAS THE SUPERVISORY AUTHORITY NOTIFIED?			**YES/NO**

IF YES, WAS THIS WITHIN 72 HOURS?	**YES/NO/NA**	
If no to the above, provide reason(s) for delay		
WAS THE BELOW INFORMATION PROVIDED? ***(if applicable)***	**YES**	**NO**
A description of the nature of the personal data breach		
The categories and approximate number of data subjects affected		
The categories and approximate number of personal data records concerned		
The name and contact details of the Data Protection Officer and/or any other relevant point of contact (for obtaining further information)		
A description of the likely consequences of the personal data breach		
A description of the measures taken or proposed to be taken to address the personal data breach (including measures to mitigate its possible adverse effects)		
WAS NOTIFICATION PROVIDED TO DATA SUBJECT?	**YES/NO**	
INVESTIGATION INFORMATION & OUTCOME ACTIONS:		
DETAILS OF INCIDENT INVESTIGATION:		
PROCEDURE(S) REVISED DUE TO BREACH:		
STAFF TRAINING PROVIDED: *(if applicable)*		
DETAILS OF ACTIONS TAKEN AND INVESTIGATION OUTCOMES:		
HAVE THE MITIGATING ACTIONS PREVENTED THE BREACH FROM OCCURRING AGAIN? *(Describe)*		

WERE APPROPRIATE TECHNICAL MEASURES IN PLACE?	**YES/NO**
If yes to the above, describe measures	
Investigator Signature: _____ Date: _____	
Investigator Name: _____ Authorised by: _____	

APPENDIX D

DEFINITIONS AND INTERPRETATION

In this Policy, the following terms shall have the following meanings:

Privacy Notice	A right to be informed, about the way in which we use, share and store personal information.
Data Protection	When you give your personal details to an organisation or individual, they have a duty to keep these details private and safe. This process is known as data protection.
General Data Protection Regulation	The General Data Protection Regulation (GDPR) came into effect on 25th May 2018 replacing current data protection laws in the European Union. The new law requires the organisation to be fully transparent to individuals and be able to demonstrate accountability for all our data processing activities.
Personal Data	Data relating to an individual who is or can be identified, directly or indirectly, 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 a person. It can be anything from a name, address, date of birth.
Processing	Doing anything with data.
Legal obligation	The processing is necessary for you to comply with the law.
Vital Interests	The processing of personal data is necessary to protect an interest which is essential for the life of the individual
Legitimate interests	The processing of personal data is necessary for the purpose of the genuine interest pursued.
Data Subject	The Data Subject is a living individual to whom personal data relates.
Subject Access Request	It is a written, signed request from an individual to see information held on them. The Data Controller must provide all such information in a readable form within 30 days.

Right to be forgotten	The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her if there are no legitimate grounds for the processing.
Data Portability	The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit that data to another controller.
Profiling & Automated Decision Making	The data subject has the right not to be subject to a decision based solely on automated processing.
Third Party	Any legal entity or person who is not the Data Controller.
Office of the Data Commissioner	The Government organisation that enforces data protection legislation. The Information Commissioner can issue Enforcement Notices and prosecute Data Controllers.
Electronic Filing	Electronic filing is a computer-based system for the storage, cataloguing and retrieval of documents. It replaces hard-copy paper documents with electronic files, which can be stored on hard drives or the cloud.