Policy / Procedure Details	Title:	**Records Management Policy for Service Users and Staff**		
	Type:	**Essential Procedure**		
	Related Personal Outcome Measure:	**I Decide When To Share Personal Information**		
	Code:	**1.21A**		
Original Version Details	Date Released:	**13/10/2011**		
Previous Version(s) Details	Date(s) Released:	**15/11/2013**	**20/ 01/2017**	**26 / 08 / 2019**
Current Version Details	Written By:	**Data Protection Officer**		
	Reviewed By:	**Procedural Review Committee**		
	Approved By:	**Procedural Review Committee**		
	Date Released:	**20/01/2020**		
	Monitoring Process:	**Procedural Review Process**		
	Date Due for Review:	**20 / 01 / 2023**		

Table of Contents

APPENDICES

Section1: Introduction

In order to plan for services effectively, to plan for future services and to ensure that a record of services provided is maintained, Western Care Association must gather and hold information on staff and each person/family using its services. Information is also gathered and maintained in relation to staff and the locations where services are provided. The organisation will ensure that the Records Management System maintains the balance between confidentiality and the obligations of the organisation in relation to the availability of information to the person using services, their families and staff who require access to information in order to do their work. The Association will comply with the General Data Protection Regulation (GDPR) and Data Protection Act and the Freedom of Information Act 2014.

Purpose
The Records Management Procedure has been developed to provide guidance for people and families using services, for staff and for people outside the Association on the following areas:

- Values and Principles in Practice; Access and Confidentiality,
- Description of types of records
- Retention periods for different types of records
- How to file and send records to the Record Management Department for safe keeping
- To set out how records are shared with people using services and families
- To set out how staff records are managed
- To describe how other service records are managed

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. The same requirement of confidentiality also applies to information about staff.

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
Each 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 the website.

In practice, consent is not sought from individuals and families in relation to the collation of personal information by support staff as part of day to day service provision. This is because it is legal requirement in order to provide safe services.

However specific consent must be sought in relation to the following instances:

1. If information is to be shared with outside agencies, i.e. schools, GMIT, CAMHS, HSE Therapists and GPs. *(See Appendix B- RMD2)*

2. If information is to be used or release for purposes outside of provision of support i.e. photographs and video recording. *(See Appendix C – RMD3)*

Function of Records and Files

The primary function of records and files are:

- To meet the legal requirements to which Western Care Association is subject to
- Necessary to comply with Employment and Revenue law
- To provide accurate, clear, comprehensive, complete, factual and concise information concerning the condition and care of the individual, and associated observations
- It is not separate from this process and it is not an optional extra to be fitted in if circumstances allow
- To provide a record of progress.
- To ensure information is regularly updated and easily retrieved
- To provide a safe and effective means of communication between members of the staff team
- To support continuity of care
- To meet legal requirements
- To form a basis of planning
- To provide written evidence of supports and service given.
- To record the chronology of events and the reason for any decisions made
- To support quality assessment and audit

The secondary functions are to provide information for:

- On-going development of services,
- The National Ability Supports System (NASS) which it used by the HSE & HRB (Health Research Board) to gather information about services individuals use and need
- Research purposes, subject to ethical considerations, and
- Responses to requests under the relevant FOI & Data Protection Acts

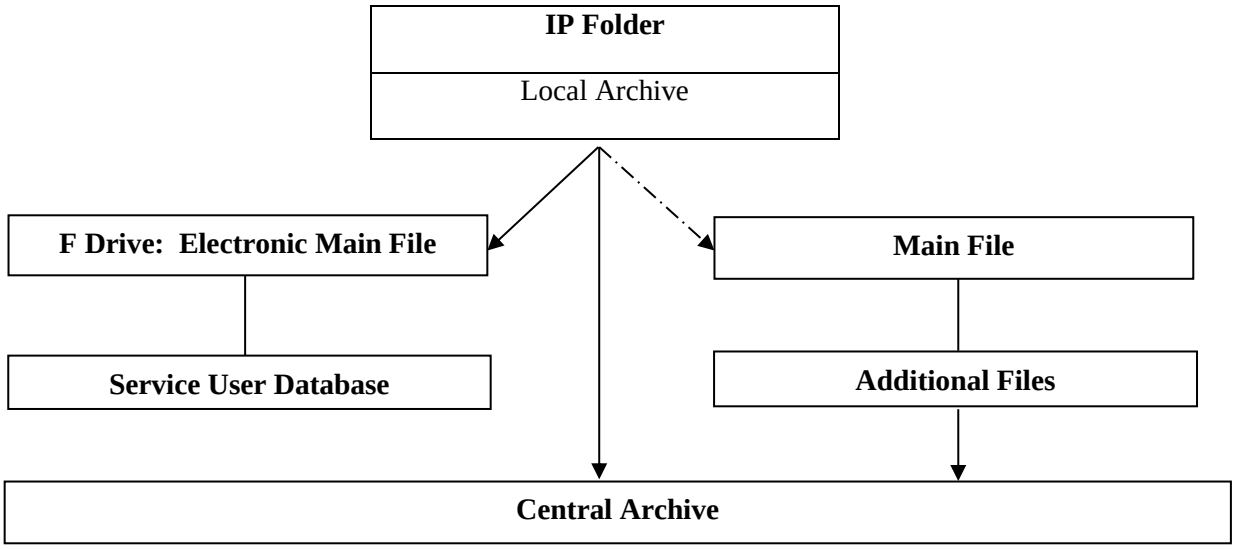
The Records Management Procedure and Process within the organisation operates within the legal obligation of the various Acts ensuring we fulfil such obligations. This policy must be read in conjunction with the Data Protection and FOI Policy which covers the following areas:

- Data Protection /General Data Protection Regulation (GDPR)
- Freedom of Information
- Informing People and Families about Records
- Access to Records
- Data Security and Breach Requirements

Section 2: Classes of Records

Records can be categorised as either related to people using services, staff or related to the particular service being provided at a given location. Classes of records are discussed in turn below.

People Using Services



1. **Individual Planning Folder (IP)**: Most people in receipt of services will have an Individual Planning Folder. The purpose of this folder is to reflect the individual's personal goals and priorities. It also details specific supports and plans in place to address those priorities. An IP is held locally with the Service User or can be accessed through the Named Staff/Regional Services Manager/Head of Service. Should a service user decide to change their services (i.e. move from a day centre to another service) their IP should always remain with them and move to the new service with them.

2. **Contents of the IP:** It is important to note that only documents currently in use for a given calendar year should be held on the folder. You can access the IP Layout on our intranet by logging onto www.westerncare.com

3. **Local Archive Folder**: The IP Folder should be cleared out once a year to remove documents such the Annual Plan or Action Plans and Progress Updates or documents that have been updated. Any photos or programme tickets referring to last year's goals can also be taken out and filed away. Therefore, each person will need to have a local archive folder where these records can be placed. Services that maintain a Link Folder will also have to maintain a Local Archive Folder to clear out this folder on a yearly basis. For ease of retrieval, it would make sense to place the records in a manila file in the Local Archive Folder firstly by year and then within each year's information use the same file structure as the IP file.
    - IP Forms
    - Daily Service Documents
    - Other Service Documents

- Incident Reports.

F Drive: **Electronic Main File:** Each person has an electronic folder, accessed through the F Drive. This is the primary electronic main file for each individual. Any document that is typed up relating to an individual must be saved to their electronic main file. When you are saving electronic records please insert a file pathname at the end of each document. This ensures that records can be located and retrieved in a timely fashion. Staff with direct access to individual's electronic record must save any document that they have created to these files. Direct access is arranged for staff working in HQ and Line Managers in frontline services.
In addition, work is in train to roll out **one additional service a Citrix license for day and adult respite services**. Frontline managers should support staff in these services to arrange a schedule for accessing this license as only one staff can access it at any one time. Further updates on progress with this project will be provided as available.

Where staff do not have access to the F drive system, frontline mangers can support staff to save service user information by using a desktop folder with subfolders for each service user. The frontline manager is then responsible for transferring across this information to each service user's F Drive folder at regular intervals.

Emails: Any email that is typed up relating to an individual must be saved to their electronic main file. It is the responsibility of the staff member who initiated the query to ensure that one copy of the completed email conversation is forwarded to the Service User electronic main file F Drive for filing. Those with access to the individual's folder can do this directly, while those who don't must ensure they forward the email to their line manager who is responsible for ensuring that it is saved to the electronic main file on the F Drive.

4. The **Main File** is a hard copy organisational file for all people using services. It should only contain referral information, legal correspondence, psychological reports and formal Psychometric Test results. As the F Drive contains electronic records of most current documents, such as IP forms, PRMP, it is not necessary to routinely copy this internally created information to Main File. The same should apply to all other file notes, signed discipline reports, signed consent forms, correspondence, including correspondences received from external resources. These should be scanned and saved to the electronic main file. The originals can be destroyed confidentially once you have them saved to the electronic file. This will ensure we do not have several duplicate copies available on the individual.

   The Frontline Manager can maintain the information in the IP file and archive from there once it has reached its retention period.

5. Each person receiving service has a record on the **Service User Database (NASS).** This record contains important information about the person's contact details and biographic information. This information is password protected and only available to Line Managers of the service in question. The Line Managers are responsible for ensuring that this information is regularly reviewed and updated as required. Changes to the database fields much be sent to Records Management by email or using the **Notification of Changes to Database Form** ***(****Appendix D - RMD 4)*

6. All records relating to people using services are maintained by the organisation indefinitely while a person is in receipt of services. Records are destroyed after a period of 20 years, once a person has ceased receiving services and after 8 years if the person dies. Therefore, the Association maintains a **Central Archive** where all personal information related to people in receipt of services can be held in accordance with these timescales. As a general rule, information should be maintained in the IP Folder/Link Folder for one year, then transferred to the local Archive folder for 6 years and then sent to Records Management for archiving. Information on Main Files is also archived where relevant after 7 years. The first quarter of each year should be used as the time to archive from, i.e. each January to March, files should be reviewed and archived as required.

7. Children who are or have been in the care of Western Care under the provisions of the Child Care Act 1991, or either on a voluntary basis or under a Court Order – these records must be kept in perpetuity. If a case /file is under investigation or if there is a court case pending or has taken place all records relating to the Service User in question should be held indefinitely.

8. **Individual Financial Records:** Records are also maintained in relation to an Individual's Property and their Day to Day spending. These records are described in the Association's policy "*Regulations Concerning Service User Monies".* These records need to be held locally for 7 years and then sent to Records Management for Archiving.

9. Additional Files: In some instances, disciplines/therapists hold **Working Files,** in addition to the Main File and IP when they are involved in a case. Where this is the case, a file note should be put on the electronic main file by the therapist indicating that a working file exists and where it is located. The members of each discipline are responsible for updating the local IP folder with any relevant information. They are also responsible to inform the database to indicate their involvement with cases. If staff leave the Department, the Head of the Department must notify the database. These records are held for 7 years and then sent to Records Management for Archiving. Note: Records available in hard copy do not need to be archived if they are saved electronically to the electronic main file. The hard copies should be destroyed confidentially.

Rehabilitative Files are maintained in centres where Rehabilitative Training is being delivered. This file focuses on the training aspect of the service. This file is kept, in addition to the IP in day centres and is accessed by the person on the programme and staff in the centre.

Occasionally, **Confidential Files** must be maintained by the organisation. These files are held in the Social Work Department. Where there is a confidential file, a file note will be placed on electronic main file to reference this.

Complaint Files: Formal Complaints - where this is the case, a file note should be put on the Service Users Main file. These files are held in the Evaluation/Training Department's office.

Informal Complaints – where this is the case the information will be scanned onto the Service User F Drive. If it contains sensitive information it will be held in the Evaluation/Training Department's office.

Legal Files: These are created when the organisation is notified that a legal case has commenced. The file will be held with the Records Manager until the case is completed and it will then be sent to the Central Archive office. Where there is a legal file, a file note will be placed on the main file to reference this.

Rights Review Committee Files: Where an individual is referred to the Rights Review Committee, a working file is created by the committee. All completed checklists used by the committee are filed electronically in each person's electronic folder on the F Drive.

Autism Services: This service does not maintain a separate IP folder. Information is saved to the electronic main file.

Staff Records

Staff files are retained in the HR Department and in local services. The following sets out the types of records held within each area.

Central Records: The HR Department maintain both electronic and hard copy records in relation to the staff. The electronic record is maintained on the CORE database. An electronic file is also created as required for information relating to individual staff on the f drive

The Personnel file is maintained securely in the HR Department. The content of the Personnel File is mainly correspondence between the HR Department and the staff. It will include:

- Job specification
- Application and Curriculum Vitae
- References
- Garda Vetting
- Offer /acceptance letter
- Recruitment medical
- Employment records
- Contract of employment
- Record of Disciplinary Action

The HR Department also maintains a range of information in relation to recruitment and industrial relations. For further information on these records and their retention, please contact the HR Department. In addition, see the staff privacy notice.

Local Service Records: The line manager should maintain a local staff file that contains information that is necessary for compliance with HIQA Regulations and the Driving for Work Policy. The HR Department facilitate each manager to have an employee file on site that will contain the following information.

- Staff Name, Address and Date of Birth
- Copy of Drivers Licence and Copy of Insurance Certificate
- Recent Photograph
- Dates he /she commenced and ceased employment (if relevant)
- Garda Vetting Information.
- Details and documentary evidence of any relevant qualifications or accredited training of the person
- Current registration status with professional bodies in respect of nursing and other health and social care professionals, if applicable
- Full employment history, together with a satisfactory history of any gaps in employment
- Relevant Correspondence between the employee, line manager and HR.
- Relevant Information from HR regarding any disciplinary action
- Support and Supervision Notes

For further information on this setting up and maintaining this file, please contact the HR Department directly. The line manager needs to maintain staff files in a secure location.

The Line Manager also has access to the electronic staff database CORE which contains a range of staff related information. It is also the main source of staff training information for Line Managers.

Complaint: Where a complaint about a staff member arises, a complaint file is held in the Evaluation/Training Department (CEO) office and/or the HR Department as applicable. When the file is retained in the CEO's office, a file note should be put on the corresponding Personnel file.

Legal Files: When the organisation is notified that a case is commenced, the HR Manager will open a "Court Case File" which will contain correspondence related to the case, including correspondence to the solicitors. This will be held within the HR Department until the case is completed. Once the court case is completed the "Court Case File" will be sent to the HR Archive. Where a legal file exists, a file note will placed on the staff file to reference this.

Location Specific Records
Line Managers are also responsible for maintaining a series of information and records related to the particular service location. These records include:

- Staff Rosters
- Staff Attendance
- Staff Training Records
- Organisational Safety Statement
- Department Safety Statement
- Emergency Plan
- Fire Drill Information
- Fire Equipment Tests
- Purchase Requisition Books
- House/Staff Diaries
- Staff Meetings Minutes
- Other Service Related Reports.
- Disposal of Medication Form

These records should be held locally for 7 years from the date of their making and then they can be forwarded for shredding as per the Association's recycling arrangements. Line Managers will need to confirm with the RSM/Head of Department regarding safe transit to the nearest collection point and keep a record in their diary of the information that was sent for shredding, the person responsible in charge at the time and the date.

Section 3: Security and Safeguarding of Records

Where files are held, a system will operate where a person will oversee the security system.

Individual Planning Folders (IPS) and Local Archive Folders
These files should be held securely based on the person's own preference. Often this may be in the person's room in the case of residential/respite supports. For people who receive Day Supports, the IP may be located in a secure office area, where the person can have access to his/her information with support.

All records relating to people using services need to be maintained for one year in a current IP Folder/Link File. They are then archived in the service for a further 6 years. Then they can be prepared as per Archiving and Retention of Records guidelines and forwarded to the Records Management Department for Archiving. *(Please refer to Section 7 - How to prepare records for Archiving)*

Main File and HR File
All Files are kept in locked filing cabinets and access to files only given where necessary.

- There is a written diary record of the name of the person who has removed the file and the date of removal.

Working Files and Additional Files
These files should be held securely when not being used.

Files must be stored in such a way that minimises the potential for deterioration and loss. They should be stored away from and protected from the hazards of fire, flooding, humidity, atmospheric pollution and vandalism.

- Secure windows
- Secure doors
- Controlled-access system
- Sturdy construction, and
- Allow protection, recovery and access to files in the event of fire or flood.

Audit of Records
It is important that regular audits of record management practice are undertaken across day, residential and respite services. To that end, a series of audit tools are attached:

- ***Record Audit Form 1 - Data Protection Officer Audit:*** This audit will be completed by the Data Protection Officer on an annual basis. Any issue identified must be followed up and addressed as soon as possible. *(See Appendix F)*

- ***Record Audit Form 2 - Frontline Manager Annual Audit:*** This audit will be completed by the frontline manager of all day, residential, IS and respite services. It reflects on key aspects of policy and training. Where issues are identified, the line manager is responsible for following up and addressing same. The Data Protection Officer is available to support managers with issues arising. Once complete please forward a copy to the Data Protection Officer and maintain a copy on site. *(See Appendix G)*

- ***Record Audit Form 3 - Frontline Manager Quarterly Audit:*** A short sampling tool has been developed to allow managers to conduct a simple check of record keeping practices at quarterly intervals. This tool focuses on the key principles of good record keeping practice and how these are in evidence in the service in the various records sample. The manager is asked to sample one of each type of record in the service as follows:

    - Service User Hard Copy: For Example IP, Archive Folders
    - Service User Electronic Copy: For Example F Drive record, any Desktop Folder if in use, Database Record
    - Staff Information Hard Copy: For Example Sample a Staff File, Volunteer File
    - Service Information Hard Copy: For Example Service Information such as Fire Drills

Once complete please forward a copy to the Data Protection Officer and maintain a copy on site. *(See Appendix H)*

Section 4: Archiving and Retention of Records

All records retained during their specified periods are traceable and retrievable. Any file movement, use or access is tracked and logged, including inter-departmental changes. All service user information is retained, stored and destroyed in line with legislative and regulatory guidelines.

Service User Records

The Service User Record Management Archival Unit is located in Head Office and our office in Ballina and is the responsibility of the Record Management Department. Two separate archival systems are in operation – one for closed records and one for records that are out of date and are no longer current to the service. A database has been set up for each system which identifies records and where they are stored.

Records are destroyed after a period of 20 years, once a person has ceased receiving services and after 8 years if the person dies. Record Management staff is responsible for the retention of these records.

Preparation of Records prior to Archiving

Prior to sending in Service User records to the Record Management Department in Head Office, staff should review the records for the following:

Duplicate Copies of Records - we need to avoid archiving duplicate copies of records. Records available in hard copy do not need to be archived if they are saved electronically to the electronic main file. The hard copy records should be destroyed confidentially.

- Staff should only send relevant records to Archives. To help determine what is a relevant record, staff should ask themselves the following questions:
- "Is this document/material necessary? i.e. if it was destroyed would it cause a gap in information? (for example, a note confirming Christmas closure dates for the centre would not be required for longer than one year)
- All Service User records should be in individual manila folders and clearly labelled on the front of the folder with the following information. Full Name/Date of Birth/Brief description of Records being Archived/time period applicable (i.e. residential records/day service records/respite records/SLT Records/Psychology Records etc.,)
- Records should be forwarded to Archives in a secure and confidential manner – (i.e. in a folder with an elastic band)
- There is no need to send in hard copies of records that are already saved to the electronic main file. These duplicate copies can be destroyed using the confidential shredding bags.

Archiving of Closed Service User Records
Closed Files are defined as records that relate to any person who no longer receives a service from Western Care Association. When a person exits our services or dies, their records are closed off and put into storage by Record Management staff or maintained in the Designated Centre. For Designated Centres, records need to be retained in the service for a period of 7 years after a resident has ceased to reside in the Service. Record Management staff will be notified of any file closure by memo, email or Database Change Form when a person dies, exits our services or no longer wishes to receive a service. The Record Management staff will forward Main File and file closure notice to the relevant member of the Management Team /Head of Department or relevant manager /staff member for signing off on the closure.

When a Service User dies Records Management will write to all those involved with the particular Service User advising that all records relating to the Service User be returned to Records Management within two weeks so the records can be updated before the file is closed. The file will then be closed and as per procedure above.
Where a service users is attending a HIQA Designated Service the Service User records will remain on site for a further for 7 years.

Local Archiving and Retention of Records for Service Users using Services
At the end of the planning year, the Named Staff reviews all documents to ensure that they are still current and updates where required. All replaced and updated documents should be filed on site in a Local Archive Folder. This information is maintained on site for 6 years and then forward to Records Management for Archiving. (Refer to section above on how to prepare records for archiving and remember we need to avoid archiving duplicate copies of records. Records available in hard copy do not need to be archived if they are saved electronically to the SU folder on the f:drive confidentially). Signed Consent Forms and the A1 Personal Information Sheet should be kept in the IP for as they are relevant and current. It is important that key planning documentation is filed securely and in sequence so that one year's worth of planning documentation is always available for review if required.

Duplication – sending records to archives. Clearly make a decision whether information needs to be held in archives. If typed – can be destroyed of as it will on the electronic file, exemptions to this would be any written record e.g. daily log.

IP Data – Held in Services		**Personnel Responsible**
Current Year's IP	Held in Service	FLM
Previous 6 Year's IP	Held in archived in the Service. Sent to Records Management for archiving after 7 years	FLM

Individual Financial Records – Held in Services		**Personnel Responsible**
Current Year	Held in Service	FLM
Previous 6 Year's	Held in archived in the Service. Sent to Records Management for archiving after 7 years	FLM

Archiving of Staff Records and Location Specific Information
All records retained during their specified periods are traceable and retrievable. Any file movement, use or access is tracked and logged, including inter-departmental changes. All company and employee information is retained, stored and destroyed in line with legislative and regulatory guidelines.

Record	Content	Retention Policy	Person Responsible
Local Staff Information	Local Staff File	This information needs to be held in respect of each staff while they are in employment at the service location and for 7 years after they cease to be in employment in that service. At that stage, the line manager should contact the HR Department for advice with regards to further archiving or destruction in each case.	FLM
Location Specific Information	Staff Rosters Staff Attendance Staff Training Records Organisational Safety Statement Department Safety Statement Emergency Plan Fire Drill Information Fire Equipment Tests Purchase Requisition Books House/Staff Diaries Staff Meetings Minutes Other Service Related Reports. Disposal of Medication Form	Keep on site for 7 years after the creation of the record. Then contact the RSM/Head of Department regarding secure transit of record to collection point for recycling as per the Association's arrangements. Maintain a local record of any information forwarded in this way.	FLM

Central Personnel File
Pension records are retained for 7 years following the normal retirement age of 65 years.
All other records are retained for 7 years following retirement or resignation of staff and then destroyed. HR personnel are responsible for the destruction of these files and keeping a log of files destroyed.

Volunteer File
This information needs to be held in respect of each volunteer while they are volunteering at the service location and for 7 years after they cease to volunteering. The Frontline Manager must inform the Volunteer Co-coordinator when a volunteer leaves a service. The Frontline Manager and Volunteer Co-ordinator is responsible for the destruction of these files.

Working Files

Record	Departments	Retention Policy	Person Responsible
Working Files /Additional Files	Psychology Speech & Language Therapy Social Work Behavior Support Physiotherapy Occupational Therapy	Sent to Records Management for Archiving after 7 years	Each Discipline

Retention of Additional Records

Record	Departments	Retention Period	Person Responsible
Inappropriate Referrals	Record Management	Destroy after 2 years once considered inappropriate	Record Management
Record of Residents	Finance	Hold for the current year plus the previous year	Head of Finance
Confidential Files Active Service Users	Social Work	Held indefinitely	Social Work
Confidential Files Service Users - closed to Western Care	Social Work	Held indefinitely in the archive unit	Social Work will forward these files to the Records Department for archiving
Assessment of Need (children not known to WCA)	Psychology	Destroy after 1 year following the completion of assessment	Admin to Head of Psychology
Drivers Time Sheets	Transport	Hold for the current year plus and previous year	Transport Manager
Company Registers		Hold indefinitely	
Development	Door to Door Envelopes	Hold for 1 year	Development Officer
Development /Fundraising	Registration forms Sponsorship Cards	Hold for 1 year	Development Officer /Fundraising Manager

Section 5: Destruction of Records

In Western Care Association, records that reach their retention period are destroyed by a recycling company by means of shredding.

At the start of each year, the Records Management Department will carry out the exercise of identifying all Service User's records that have reached their retention period. These records are then placed in recycling bags and collected by the recycling company. The date of destruction is recorded on the closed database by the Records Management Department. The Records Management staff will inform the CEO in writing of the files for destroying prior to their destruction.

Where staff records have reached the timeframe for removal from the local centre, the line manager should contact the HR department for advice on how to proceed. For location specific records, they can be forwarded for shredding as per the Association's recycling arrangements. Line managers will need to confirm with the Regional Services Manager regarding safe transit to the nearest collection point and keep a record in their diary of the information that was sent for shredding, the person responsible in charge at the time and the date.

Section 6: Staff Training Awareness on Record Management and GDPR

Each staff member must complete some form of GDPR training. Frontline Managers are responsible for ensuring that all their staff receives GDPR training.

Some staff will have completed the Staff Awareness Training through Privacy Engine. However, this option is no longer available to us. Therefore, new staff must complete the HSEland Online GDPR training module. On completion, the certificate of achievement should be forwarded to the Evaluation & Training Department for recording purposes.

In addition, the Data Protection Officer will brief each new Frontline Manager on this policy as part of their induction to the organisation. The Frontline Manager will also need to complete the online training following this briefing.

The Data Protection Officer will attend Area Team meetings annually to remind staff of their obligations when processing personal data and ensuring compliance with policy.

A PowerPoint presentation on Records Management /GDPR will also be available on the intranet for Frontline Managers, which they should use as a refresher at their staff team meeting on an annual basis. They also have the option of using the HSEland Online training module if they prefer. Either way, is it important that GDPR is discussed annually at staff team meetings.

The Data Protection Officer will be available to you to answer any queries regarding this policy and training options available to you.

Section 7: Best Practice in Records Management

Keeping a Clear Desk. Staff should never leave personal or sensitive information on their desks unattended or in any area that it may be seen or accessed by an unauthorised person. At the end of each day staff must lock away all personal and sensitive information.

Saving Electronic Records. When you are saving electronic records please insert a file pathname. A guidance document to explain this process is available with this policy. Implementing this practice ensures that records can be located and retrieved in a timely fashion. It also reduces the proliferation of duplicate copies of documents and will help when it comes to archiving paper records.

Printing to the Photocopier in HQ. If you are printing confidential information you must use the "secure print" option on your computer. Those documents will be held in the memory of the machine and can only be printed as and when you enter your password into the printer. This way, confidential documents are not left lying around for everyone to access.

Scanning documents on the Photocopier in HQ. When scanning confidential information, you should use the "encryption" option mode on the printer. When print jobs are scanned in this mode, those documents can only be retrieved from the scan folder by entering a password. This way, only the person who scanned the document can open it.

Communicating externally through E-mail.
The use of personal email accounts for the transmission of Western Care information is strictly prohibited.

For security reasons users must not forward their Western Care email messages to their own personal email account.

E-mails can be retrieved, examined, and used in a court of law. Information on Service Users can only be transferred electronically if the file (attachment) is password protected. The password used to read the attachment must not be sent along with the original e-mail message.

Once you have sent the password protected document you will need to remove the password from the actual document. This is important as the document may need to be accessed at a later date.
The body of the e-mail should not contain any identifiable information either that could potentially identify a Service User.

Making a telephone call using loud speaker
If you are using the speakerphone to answer /make telephone calls your office door must be closed to avoid unauthorised disclosure of personal data.

Travelling Files

Information travelling on a regular basis is a security risk as it may potentially get lost and come into the possession of person unauthorised to have that information. The organisation is considering methods of enhancing electronic solutions in order to reduce the risks in this area. However, at present, it is important to manage the risks through the streamlining of current practices in this area through the safeguards set out below.

- Each line manager is responsible for the managing of the risks associated with the regular transit of service user information between services and other services and/or home.
- Where possible electronic copies should be circulated using the f drive system. This is particularly apt where it is a document that is not subject to regular change. (For example protocols, guidance, PRMPs)
- Only required information travels. This should be critical information, usually about the person's day. It may include a daily log, medication recording details, seizure records.
- Where information is travelling, the manager should ensure it is stored safely in transit and that an assigned staff member is responsible for both handing it over for transit and a responsible person is responsible for receiving it at its destination.
- Any accidental loss of travelling information is a data breach and needs to be reported accordingly, see Data Protection Policy, Section 5.
- Given the risks associated with this practice, it should receive a specific focus in the regular audits of record practices conducted by the manager and follow up action taken where required.
- Often buses/transport associated with services will have a transport emergency plan on board. The manager should ensure this is placed in a secure location on the vehicle. The vehicle must be locked at all times when not in use.
- Community Based Staff should ensure that service user records/folders are securely stored in the boot of your car when travelling.
- Main files travelling between HQ and the Ballina office should be secured in a locked briefcase and only transported by staff going direct to the location.
- If arranging for the transportation of information either for archive or shredding, please contact either your RSM/Head of Department or the Data Protection Officer.

Removing Records from On-site

Users must not remove any confidential information (irrespective of format) from the facility they are employed at without the authorisation of their line manager. Such authorisation must be issued in advance of the first instance and may apply thereafter if necessary. Where a user has been authorised to remove confidential or restricted information from a Western Care facility they will be responsible for the safe transport and storage of the information i.e. locked in the boot of your car during transit and in locked storage when not in use.

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.

(RMD 2)

CONSENT FORM FOR RELEASE OF RECORDS TO AN OUTSIDE AGENCY

DATE [ ]

I/WE _____ GIVE PERMISSION TO [staff member & Service Location] _____ TO RELEASE THE FOLLOWING DOCUMENTS/RECORDS [outline description & data of records]

_____

_____

_____

_____

TO [name of agency/person _____

For the Purpose of: _____

I consent to the above YES ☐

I do not consent to the above NO ☐

Signed: _____ Date: _____

This form is to be used if information is to be shared with an outside agency, i.e. schools, GMIT, CAMHS, HSE Therapists, GPs, etc.

(A copy of this should be held on file)

(RMD 3)

CONSENT FORM

FOR ACCESSING INFORMATION FOR A SPECIFIC PURPOSE

(Examples: use of photographs, video recording, etc.)

NAME OF PERSON/FAMILY:_____

SERVICE: _____

Name(s) of the Person(s) requiring consent:

_____

State the purpose for requiring consent from this person/family:

_____

State what the information will be used for?

_____

_____

How long is the consent required?
(Is this just required for a specific time period for example Personal Outcomes Interview or is it long term)

Please state the time period for which the consent is required:

_____

I consent to the above YES ☐

I do not consent to the above NO ☐

Signature of Person/Family: _____ Date: _____

(A copy of this should be held on file)

(RMD 4)

Western Care Association
NOTIFICATION OF CHANGES TO SERVICE USER DATABASE

1. SERVICE USER'S NAME & ADDRESS	*DATE OF BIRTH*

2. NAME OF FIELD TO BE UPDATED *i.e. Contact Number (Primary);Main Service Name*	*3. DETAILS OF CHANGE*

4. PERSON REQUESTING CHANGE

*Signature*_____ *Date*_____

5. REGIONAL SERVICE MANAGER/HEAD OF DEPARTMENT

*Signature*_____ *Date*_____

For administration/record management use only

6. Fields updated

*Signature*_____ *Date*_____

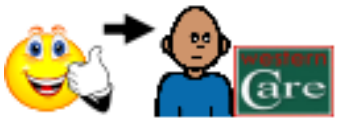
NOTE – ***This form should be used to record changes to the Service User database.***

If a Service User/parent/guardian dies this from should be completed immediately and sent to the Record Management department in Castlebar

Western Care Association

CONSENT LETTER FOR RELEASE OF RECORDS TO OUTSIDE AGENCY

I/We



give permission to (staff member and work location)

to release the following documents/records (outline description of records)

to (name of agency/person)

Signed:

Dated:

DISCLAIMER
Western Care Association ceases to accept responsibility for the safeguard of the above specified documents/records once released to any outside agency or individual.

Western Care Association

"I choose when to share information about me"

Request for Service User/Family to access Main File

Part A—to be completed by Named Staff / Service User

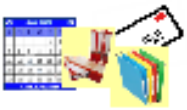
Name & contact number:

Date:

Named Staff:

Any special requirements (i.e. tape recorder/camera):

Part B—to be completed by FOI Officer



Date received by FOI Officer:

Date file checked by Decision Maker:

Date/time of visit arranged:

Did visit take place? 

If **No**, new date and time arranged for visit:

Record Management will try and facilitate all requests within 2 working weeks, where possible.

For Main Files held in the North (Ridgepool Office) please allow 3 weeks, as the Freedom of Information Officer is located in Head Office.

Please note: the Freedom of Information Officer is available from 9.30 a.m. — 1.00 p.m. and from 2.00 p.m. — 4.00 p.m. and visits should be arranged during this time.

Western Care Association

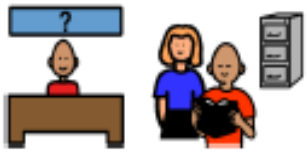
CONSENT FORM

For accessing information for a specific purpose

Name of person/family:

Service:

Name(s) of the person(s) requiring consent:



State what the information will be used for:

How long is the consent required? (for a specific time period, e.g. Personal Outcomes Interview, or is it long term? Please state the time period for which consent is required:

I/we

Give permission to release the following documents/records (outline description of records)

Date: _____

Audit Form 1 - Data Protection Officer Audit

A: Organisation Level – To be completed by DPO annually			
Question	**Answer**	**Comment**	**Evidence should be seen, as appropriate, and recorded as such**
Do you have a copy of the IT Policy, Data Protection Policy & Records Management Policies available to staff?			
Has all staff signed documentation stating they have read and understood these policies?			
How are you notified of any updates, changes in practice?			
How are managers and front line staff notified of the updates of the Policies, Procedures & Guidance (PPG's)			
Has the organisation access to a Data Protection Officer?			
Do you know who your Data Protection Processors are?			
How many annual requests under Data Protection did WCA receive?			

Reporting Breaches			
Question	**Answer**	**Comment**	**Evidence should be seen, as appropriate, and recorded as such**
Do you have written procedures informing staff as to how to respond when a data breach is suspected or occurs?			
Do you have written procedures informing frontline staff how to report concerns about a Data Protection breach?			
Were there any data breaches reported in this period?			
Did you inform the data subject (s) and the Office of the information Commissioner			
Investigating a Breach			
Question	**Answer**	**Comment**	**Evidence should be seen, as appropriate, and recorded as such**
Do you have procedures for investigating a Data protection breach?			
When are cases reported to the Data Protection Officer?			
When are cases reported to the Data Protection Commissioner?			

How do you close the loop from when an alleged incident is disclosed until closure?			
Responsibility and Recording			
Question	**Answer**	**Comment**	**Evidence should be seen, where appropriate, and recorded as such**
Did you brief new FLM's on Record Management & GDPR as part of their induction?			
Did you attend any Area Team Meetings to discuss GDPR /Records Management during this period?			
Do you have an identified person who is responsible for keeping a log of data processing activities?			
What is their role in the organisation?			
How often are these activities monitored?			
Do you have a risk register in place where there is a risk associated with the processing activity?			
Who is responsible for maintaining this register?			
Are risks on this register communicated to those involved for follow up?			
Any other issues in relation to GDPR /Record Management			

Organisational Training in Data Protection			
Question	**Answer**	**Comment**	**Evidence should be seen, as appropriate, and recorded as such**
Is the HSEland GDPR online training being rolled out to all new staff?			
Is there a training database/register?			
How often is training delivered to staff?			
Are training certificates issued and where are these held?			
Audit			
Question	**Answer**	**Comment**	**Evidence should be seen, as appropriate, and recorded as such**
Did FLM's carry out quarterly audits of service user, staff & service information records? Were you provided with this data?			
Did the DPO carry out any service audit during this period?			
Are audit reports & data breaches reported the CEO and the Board on annual basis?			

Signed: _____ Date: _____

Audit Form 2 – Frontline Manager Annual Audit

Form to be Copied and Sent to DPO with Copy to be Held on Site.			
Question	**Answer**	**Comment**	**Evidence should be seen, as appropriate, and recorded as such**
Do you have a copy of the IT, Data Protection and Records Management Policies available to staff?			
Do you have a Policy folder available in your service?			
Have you signed documentation stating that your team have read and understood the policies?			
How are you notified of updates, changes in practice to the Policies and Procedures?			
Has the privacy notices been made available to individuals?			
If you have questions about Data Protection, who would you ask?			
Do you have access to a local person who knows about Data Protection?			
Has anyone approached you in relation to a Data Protection issue, i.e. staff, individual using services, family members?			
If they have who did you notify?			

Reporting Breaches			
Question	**Answer**	**Comment**	**Evidence should be seen, as appropriate, and recorded as such**
Do you know what a data Breach is			
Do you have and understand any written procedures informing you as to how to respond when a data breach is suspected or occurs?			
Did you have any breach in your service this period?			
Did you report the breach to the DPO?			
Responsibility & Recording			
Question	**Answer**	**Comment**	**Evidence should be seen, where appropriate, and recorded as such**
Are there any areas in the attached policy that are proofing problematic for your service to comply or causing you concern?			
Do you have a system to record Data Protection information?			
Do you have a system for creating and recording information on files?			
Are there any issues around GDPR you need addressed at this time?			
Have you informed the DPO of these issues?			

Organisational Training and Awareness in Data Protection			
Question	**Answer**	**Comment**	**Evidence should be seen, as appropriate, and recorded as such**
Have staff access to copies of the relevant policies?			
Did you discuss GDPR at your staff team meeting this year?			
Has all your staff team completed some form of GDPR training (either through Privacy Engine /HSEland)			
Have you addressed the gap in training with those Individuals to ensure completion?			
Do you keep a register in your service of those who have completed this training?			
Are training certificates being sent to ETD for record keeping?			

Audit				
Question	**Answer**	**Comment**	**Evidence should be seen, as appropriate, and recorded as such**	
Have you any issues in relation to the processing of records in your service?				
Security and confidentiality is adequate to prevent unauthorised access to records?				
Are you aware of the procedure for archiving of records and their retention periods?				
Is there a dedicated area in your service for the archival of records?				
Are archived records stored securely?				
Please insert the dates of Quarterly Records Audits Completed in your Service this past year?	***Date Audit Q1:***	***Date Audit Q2:***	***Date Audit Q3:***	***Date Audit Q4:***
Summarise if there were issues arising and the follow up completed as a result:				
Audit Completed By: ***Date Completed:***				

Audit Form 3: Frontline Manager Quarterly Audit **Form to be Copied and Sent to DPO with Copy to be Held on Site.**	
Name of Service:	Quarter/Year:
Please tick record audited ☐ Service User Hard Copy, e.g. Individual Plan ☐ Service User Electronic, e.g. F Drive Record or Desktop File ☐ Staff Information Hard Copy, e.g. staff file ☐ Service Information Hard Copy, e.g. fire drill records	
Describe the Information Checked?	
Why is this information collected?	
Is the Information Accurate?	
Is it Secure and Confidential? E.g Accessed only by those with Permission to do so?	
Is it Shared or Travelling outside the Service Appropriately?	
Is it retained in line with the policy guidance on Retention?	
Any Other Issue Arising with this Record?	
Completed by:	Date: