Personal Data Security Breach Management Policy

1.0 Purpose

The Data Protection Acts 1988 and 2003 impose obligations on data controllers in Western Care Association to process personal data entrusted to them in a manner that respects the rights of data subjects (Service Users, families and employees) to have their data processed fairly. Information /data is one of our most important assets and each one of us has a responsibility to ensure the security of this information. Accurate, timely, relevant and properly protected records are essential.

Sometimes a breach of information/data security may occur because this information/ data is accidentally disclosed to unauthorized persons or, lost due to a fire or flood or, stolen as result of a targeted attack or the theft of a mobile computer device.

The purpose of this policy is to ensure that a national standardised management approach is implemented throughout the organisation in the event of an information/data breach.

This policy is mandatory and by accessing any of Western Care Association Information/data, users are agreeing to abide by the terms of this policy.

2.0 Scope

This policy applies to all employees, service providers and third parties that access, use, store or process information on behalf of Western Care Association. This policy is authorised by the Executive Director in Western Care Association.

3.0 Legislation

Western Care Association has an obligation to abide by all relevant Irish legislation and European legislation. The relevant acts, which apply in Irish law to Information Systems, include but are not limited to:

- The Data Protection Act (1988/2003)
- European Communities Data Protection Regulations, (2001)
- European Communities (Data Protection and Privacy in Telecommunications)
- Data Protection EU Directive 95/46/EC
- Criminal Damages Act (1991)

4.0 Policy

It is the policy of Western Care Association that in the event that an information/data breach happens, the following breach management plan is strictly adhered to.

It is important that each manager puts into place their own local procedures to enable them to implement the breach management plan should such a data breach occur. There are five elements to any breach management plan:

- Identification and Classification
- Containment and Recovery
- Risk Assessment
- Notification of Breach
- Evaluation and Response

5.0 Breach Management Plan

5.1 Identification and Classification

Senior Management must put in place procedures that will allow any staff member to report any information/data security breach.

- It is important that all staff are aware to whom they should report such a breach. You must report any breach of information /data to your manager as soon as you detect it.

- Having such a procedure in place will allow for early recognition of the breach so that it can be dealt with in the most appropriate manner.

- Details of the breach should be recorded accurately by the person who detected the breach or their manager. You must include the date and time the breach occurred, the date and time it was detected, who reported the breach, description of the breach, details of any computer systems involved and forwarded to the appropriate Manager. (See Form attached).

- In this respect, staff need to be made fully aware as to what constitutes a breach. In respect of this policy a breach maybe defined as the unintentional release of confidential or personal information/data to unauthorised persons, either through the accidental disclosure, loss or theft of the information/data.

5.2 Containment and Recovery

Containment involves limiting the scope and impact of the breach of data/information.

If a breach occurs, management should:

- Decide on who would take the lead in investigating the breach and ensure that the appropriate resources are made available for the investigation.

- Establish who in the organisation needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. For example, finding a lost file.

- Establish whether there is anything that can be done to recover losses and limit the damage the breach can cause.

5.3 Risk Assessment

In assessing the risk arising from the security breach, managers should consider what would be the potential adverse consequences for individuals, i.e. how likely it is that adverse consequences will materialise and, in the event of materialising, how serious or substantial are they likely to be. In assessing the risk, managers should consider the following points:

- What type of Information/data is involved?
- How sensitive is the information/data?
- Are there any security mechanism's in place (e.g. password, protected, encryption)?
- What could the information/data tell a third party about the individual?
- How many individuals' are affected by the breach?

5.4 Notification of Breaches

- If the data concerned is protected by technological measures such as to make it unintelligible to any person who is not authorised to access it, the data controller may conclude that there is no risk to the data and therefore no need to inform data subjects. Such a conclusion would only be justified where the technological measures (such as encryption) were of a high standard.
- All incidents of loss of personal data in manual or electronic form by a data processor must be reported to their manager /relevant data controller as soon as the data processor becomes aware of the incident.
- All incidents in which personal data has been put at risk should be reported to the Office of the Data Protection Commissioner as soon as the data controller becomes aware of the incident, except when the full extent and consequences of the incident has been reported without delay directly to the affected data subject(s) and it affects no more than 100 data subjects and it does not include sensitive personal data or personal data of a financial nature.
- Data controllers reporting to the Office of the Data Protection Commissioner in accordance with this policy should make initial contact with the Office within two working days of becoming aware of the incident, outlining the circumstances surrounding the incident. This initial contact may be by e-mail (preferably), telephone or fax and must not involve the communication of personal data. The Office of the Data Protection Commissioner will make a determination regarding the need for a detailed report and/or subsequent investigation based on the nature of

the incident and the presence or otherwise of appropriate physical or technological security measures to protect the data.

- Should the Office of the Data Protection Commissioner request a data controller to provide a detailed written report of the incident, the Office will specify a timeframe for the delivery of the report based on the nature of the incident and the information required. Such a report should reflect careful consideration of the following elements:
    - the amount and nature of the personal data that has been compromised
    - the action being taken to secure and / or recover the personal data that has been compromised;
    - the action being taken to inform those affected by the incident or reasons for the decision not to do so;
    - the action being taken to limit damage or distress to those affected by the incident;
    - a chronology of the events leading up to the loss of control of the personal data; and the measures being taken to prevent repetition of the incident.
- Depending on the nature of the incident, the Office of the Data Protection Commissioner may investigate the circumstances surrounding the personal data security breach. Investigations may include on-site examination of systems and procedures and could lead to a recommendation to inform data subjects about a security breach incident where a data controller has not already done so. If necessary, the Commissioner may use his enforcement powers to compel appropriate action to protect the interests of data subjects.
- Even where there is no notification to the Office of the Data Protection Commissioner, the data controller should keep a summary record of each incident which has given rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data. The record should include a brief description of the nature of the incident and an explanation of why the data controller did not consider it necessary to inform the Office of the Data Protection Commissioner. Such records should be provided to the Office of the Data Protection Commissioner upon request.

5.5 Evaluation and Response

- Subsequent to any information/data security breach a thorough review of the incident should occur. The purpose of this review is to ensure that the steps taken during the incident were appropriate and to identify areas that may need to be improved.

- Any recommended changes to policies and/or procedures should be documented and implemented as soon as possible thereafter.

Senior Management should identify a group of people within the organisation who will be responsible for reacting to reported breaches of security.

6.0 Roles and Responsibilities

6.1 Line Managers

Managers are responsible for:

- The implementation of this policy.
- Ensuring that all employees who report to them are made aware of and are instructed to comply with this policy and all other related policies.
- Agreeing the appropriate procedures to follow when a breach of this policy has occurred.

6.2 Users

Each user is responsible for:

- Complying with the terms of this policy and all other relevant Western Care policies, procedures, regulations and applicable legislation;
- Respecting and protecting the privacy and confidentiality of the information they process at all times;
- Reporting all misuse and breaches of this policy to their manager.

7.0 Enforcement

Western Care Association reserves the right to take such action as it deems appropriate against users who breach the conditions of this policy. Western Care Association employees who breach this policy may be denied access to the organisations information technology resources, and maybe subject to disciplinary action.

8.0 Review & Update

This policy will be reviewed and updated annually or more frequently if necessary, to ensure that any changes are properly reflected in the policy.

Details of Data Security Breaches

DATE & TIME BREACH OCCURED	DATE & TIME BREACH DETECTED	WHO REPORTED THE BREACH	DESCRIPTION OF THE BREACH	DETAILS OF ANY COMPUTER SYSTEMS INVOLVED

Signed: _____ Date: _____

Name & Tile of Person Completing Form

Once completed please forward to your Manager.