

WEST LIMERICK INDEPENDENT LIVING CLG
Data Breach Response Policy

Policy Reference	WLILP7B
Category	Operational Policies — Data Protection (2 of 4)
Version	2.0 (role-based contacts, cross-referenced)
Status	APPROVED — by the Board of Directors on 9 October 2026
Supersedes	WLILP10 - Data Breach Response Policy
Series	Second of four data protection policies — see WLILP7A - Data Protection Policy for overarching principles and the Data Protection Officer's role.
Policy Owner	Board of Directors, West Limerick Independent Living CLG
Applies To	All employees, contractors, volunteers, and third parties handling personal data on behalf of WLIL
Related Policies	WLILP7A - Data Protection Policy; WLILP7C - Data Access (Subject Access Request) Policy; WLILP7D - Data Retention, Rectification and Erasure Policy
Review Cycle	Annually, or sooner following a significant breach or a change in legislation

1. Purpose and Scope

This policy establishes clear procedures for identifying, managing and reporting personal data breaches, in compliance with GDPR and the Data Protection Act 2018. It applies to all employees, contractors, volunteers and third parties handling personal data on behalf of West Limerick Independent Living CLG ("WLIL").

2. Legislative Framework

- General Data Protection Regulation (EU) 2016/679 (GDPR), Articles 33 and 34
- Data Protection Act 2018 (Ireland)
- Guidance issued by the Data Protection Commission (DPC)

3. Definition of a Data Breach

A data breach is any incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, whether transmitted, stored, or otherwise processed. Examples include:

- loss or theft of a device containing personal data
- sending personal data to the wrong recipient
- unauthorised access to systems or files
- loss of paper records containing personal information

4. Policy Statement

WLIL is committed to protecting the personal data of service users, staff and stakeholders. All suspected or confirmed data breaches must be reported immediately, managed effectively, and, where necessary, reported to the Data Protection Commission within 72 hours. High-risk breaches will also be communicated to affected individuals without undue delay.

5. Procedures

5.1 Identifying a Breach

- Any staff member who suspects or identifies a data breach must immediately notify their line manager and the Data Protection Officer (DPO)

5.2 Containing a Breach

- Take immediate steps to contain the breach — for example recalling emails, disabling compromised accounts, or securing records

5.3 Reporting Internally

- Complete a Data Breach Report Form (Appendix A) and submit it to the DPO within 24 hours

5.4 Risk Assessment

- The DPO will assess the severity of the breach using the Incident Log (Appendix B)

5.5 Notification to the DPC

- Where there is a risk to individuals' rights, the DPO will notify the Data Protection Commission within 72 hours using the template in Appendix C

5.6 Notification to Individuals

- If the breach presents a high risk, the DPO will notify affected individuals promptly using the template in Appendix D

5.7 Corrective Action

- Lessons learned and corrective measures will be documented and implemented
- Staff retraining or disciplinary action may be required where breaches arise from negligence

6. Roles and Responsibilities

- All Staff — report suspected breaches immediately and cooperate with investigations
- Line Managers — support reporting staff and assist with containment
- Data Protection Officer — leads investigations, maintains records, and notifies the DPC and affected individuals where necessary (see WLILP7A, Section 5, for the DPO's role generally)
- Board of Directors — provides oversight and ensures accountability

7. Training and Awareness

All staff receive data protection and breach reporting training during induction, with annual refresher training. Additional training is provided following any significant breach.

8. Monitoring and Review

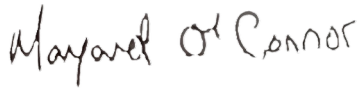
This policy will be reviewed annually by the DPO, or sooner if required by changes in legislation, regulatory guidance, or following a significant breach. Non-compliance with this policy may result in disciplinary action.

This policy reflects GDPR Articles 33 and 34 and the Data Protection Act 2018, checked as accurate as of drafting.

Approval

Approved by the Board of West Limerick Independent Living CLG on 9 October 2026.

Signed on behalf of the Board, on its instruction, by the General Manager:



Margaret O'Brien O'Connor, General Manager

Date signed: 09-10-2026

Appendix A — Data Breach Report Form

Date of Breach: _____

Reported By (role): _____

Location: _____

Description of Breach:

Data Affected:

Immediate Action Taken:

Reported To (Manager/DPO): _____ Date: _____

Signature: _____

Appendix B — Incident Log Register

A log of all breaches must be maintained, including:

- Date and time of breach
- Description of incident
- Individuals/data affected
- Containment actions taken
- Risk assessment outcome
- Notification status (DPC/individuals)
- Corrective actions implemented

Appendix C — Notification Template (Data Protection Commission)

Subject: GDPR Data Breach Notification

To: Data Protection Commission

We are notifying you of a personal data breach in compliance with Article 33 of the GDPR.

- Date and time of breach:
- Nature of personal data involved:
- Categories and approximate number of data subjects affected:
- Categories and approximate number of records concerned:
- Likely consequences of the breach:
- Measures taken to address/mitigate the breach:

Contact details of DPO (role): _____

Signed: _____ Date: _____

Appendix D — Notification Template (to Affected Individuals)

Subject: Important Notification — Personal Data Breach

Dear [Name],

We regret to inform you that a personal data breach occurred on [Date]. The breach involved [summary of data affected]. We have taken the following steps to contain the breach and protect your information:

- [List of corrective measures taken]

Please be vigilant for any unusual activity relating to your personal data and contact us if you require further information. You have the right to lodge a complaint with the Data Protection Commission.

Contact details of Data Protection Officer (role): _____

Sincerely, WLIL Data Protection Officer

Appendix E — Staff Acknowledgement Form

I acknowledge that I have read and understood WLIL's Data Breach Response Policy. I agree to comply with its requirements and understand that failure to do so may result in disciplinary action.

Name: _____

Signature: _____ Date: _____