

WEST LIMERICK INDEPENDENT LIVING CLG

Data Protection Policy

Policy Reference	WLILP7A
Category	Operational Policies — Data Protection (1 of 4)
Version	3.1 (CCTV and visual monitoring added as Section 11)
Status	APPROVED — by the Board of Directors on 9 October 2026
Supersedes	WLILP7 - Data Protection Policy 2024 A
Series	This policy is the first of four documents forming WLIL's data protection suite: WLILP7A (this policy — principles and governance), WLILP7B (Data Breach Response), WLILP7C (Data Access / Subject Access Requests), WLILP7D (Data Retention, Rectification and Erasure). The Board should retire the old numbers WLILP10, WLILP26 and WLILP27 once this set is approved, to avoid two numbering schemes for the same documents.
Policy Owner	Board of Directors, West Limerick Independent Living CLG
Applies To	All staff, contractors, volunteers, and any third party processing personal data on WLIL's behalf
Related Policies	WLILP7B - Data Breach Response Policy; WLILP7C - Data Access (Subject Access Request) Policy; WLILP7D - Data Retention, Rectification and Erasure Policy; WLILP29 - Information Systems and Cloud Access Control Policy; WLILP19 - Lone Working Policy; WLILP50 - Travel and Subsistence Policy; WLILP28 - Clean Desk Policy; WLILP55 - Disciplinary Policy; WLILP56 - Grievance Policy
Review Cycle	Annually, or sooner if legislation or guidance changes

1. Introduction

West Limerick Independent Living CLG ("WLIL") needs to gather and use certain information about individuals, including service users, funders, business contacts, employees and other people the organisation has a relationship with. This policy describes how this personal data must be collected, handled and stored to meet WLIL's data protection standards and to comply with the law.

This is the first of four related policies. This policy sets out WLIL's overarching principles and governance; WLILP7B, WLILP7C and WLILP7D set out the specific procedures for breach response, subject access requests, and retention/rectification/erasure respectively. Staff needing to act on a specific data protection matter should go to the relevant procedure document directly.

2. Legislative Framework

- General Data Protection Regulation (EU) 2016/679 (GDPR) — replaced the EU Data Protection Directive 95/46/EC and applies directly across the EU
- Data Protection Act 2018 (Ireland) — gives further effect to GDPR in Irish law

- Guidance issued by the Data Protection Commission (DPC)

The GDPR's territorial scope (Article 3) applies to all controllers established in the EU processing personal data in that context, and to controllers outside the EU offering goods or services to, or monitoring the behaviour of, people in the EU.

3. Key Definitions (GDPR Article 4)

Personal data: any information relating to an identified or identifiable living individual (a "data subject")

Special category data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, health data, or data concerning sex life or sexual orientation

Data controller: the person or body which determines the purposes and means of processing personal data — WLIL is a data controller in respect of the personal data of its service users, staff and others

Data processor: a person or body which processes personal data on behalf of a controller — WLIL may also act as a processor in some contexts, and engages processors itself (for example, IT service providers)

Processing: any operation performed on personal data, including collection, storage, use, disclosure, or destruction

Personal data breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data — see WLILP7B for WLIL's breach response procedure

Data subject consent: a freely given, specific, informed and unambiguous indication of the data subject's wishes, by a statement or clear affirmative action, signifying agreement to processing

A child, for GDPR purposes, is defined as under 16; the processing of a child's personal data on the basis of consent requires parental or guardian consent, and WLIL will make reasonable efforts to verify this where relevant.

4. Why This Policy Exists

- Complies with data protection law and follows good practice
- Protects the rights of staff, service users and partners
- Is open about how WLIL stores and processes individuals' data
- Protects WLIL from the risks of a data breach

5. The Data Protection Officer

WLIL has appointed a Data Protection Officer (DPO), a role specified in GDPR Article 37. Given that WLIL's core activity involves large-scale processing of special category data (health and disability-related information about service users), WLIL likely meets the mandatory DPO appointment threshold under Article 37(1)(c), rather than appointing a DPO purely as good practice — the Board should treat this appointment as a compliance requirement, not a discretionary one.

GDPR Article 38(6) requires the DPO to be able to perform their tasks independently, without being instructed on how to exercise them, and without conflicts of interest. If the person holding the DPO role is the same person as the General Manager, or another role responsible for deciding the purposes and means of WLIL's data processing, this is a recognised independence conflict — the DPO would in effect be reviewing their own

decisions. The Board should confirm the DPO is a genuinely distinct role from operational management, or put additional safeguards in place if it is not.

The DPO is accountable to the Board for WLIL's management of personal data and for demonstrating compliance with data protection legislation and good practice. The DPO's responsibilities include:

- keeping the Board updated on data protection responsibilities, risks and issues
- reviewing data protection procedures and related policies on an agreed schedule
- arranging data protection training and advice for staff and others covered by this policy
- handling data protection questions from staff and data subjects
- overseeing subject access requests (see WLILP7C) — day-to-day intake and coordination may be delegated by the DPO to the General Manager or another designated staff member, provided the DPO retains overall responsibility for compliance
- overseeing breach response (see WLILP7B)
- checking and approving contracts or agreements with third parties that may handle WLIL's personal data
- reviewing, at least annually, the retention dates of personal data processed by WLIL, by reference to the data inventory

Compliance with data protection legislation is the responsibility of every member of staff who processes personal data, not the DPO alone.

6. The Six Data Protection Principles

GDPR requires that personal data be:

- processed lawfully, fairly and in a transparent manner
- collected for specified, explicit and legitimate purposes
- adequate, relevant and limited to what is necessary
- accurate and, where necessary, kept up to date
- retained for only as long as necessary
- processed in a manner that ensures appropriate security

6.1 Lawfulness, Fairness and Transparency

Data subjects must be given clear information about WLIL's identity and contact details, the DPO's contact details, the purpose and legal basis of processing, how long data will be held, their rights, and any third-country transfers. This information is provided in a privacy notice given to individuals at the time their personal data is collected. As a not-for-profit organisation, WLIL only uses personal data to provide personal support services and related administration.

6.2 Purpose Limitation

Data obtained for a specified purpose must not be used for an incompatible purpose. The DPO is responsible for ensuring WLIL does not collect information beyond what is strictly necessary, and that data collection forms include a fair processing statement or link to the privacy notice.

6.3 Data Minimisation

Data collection methods will be reviewed at least annually to ensure collected data remains adequate, relevant and not excessive.

6.4 Accuracy

Data must be reviewed and updated as necessary; no data should be kept unless it is reasonable to assume it is accurate. It is also the responsibility of the data subject to ensure data WLIL holds about them is accurate and current.

6.5 Storage Limitation

Personal data will be retained in line with WLILP7D - Data Retention, Rectification and Erasure Policy and, once its retention date passes, must be securely destroyed. Where retention beyond that policy's standard periods is genuinely needed, the DPO must specifically and separately approve this in writing, with a documented justification.

6.6 Integrity and Confidentiality (Security)

In determining what security is appropriate, the DPO considers the possible harm to individuals from a breach, the effect on WLIL, and any reputational risk. Technical measures considered include:

- password protection and automatic locking of idle terminals
- removal of access rights for USB and other removable media where not required
- virus checking software and firewalls
- role-based access rights, including for temporary staff
- encryption of devices that leave WLIL's premises, such as laptops
- security of local and wide area networks
- privacy-enhancing techniques such as pseudonymisation and anonymisation, where appropriate

Organisational measures considered include staff training, reference checks, inclusion of data protection obligations in employment contracts, disciplinary measures for breaches, physical access controls, a clean desk approach (see WLILP28), lockable fireproof storage for paper records, restrictions on personal devices, clear password rules, and regular off-site backups. See WLILP29 - Information Systems and Cloud Access Control Policy for the detailed technical implementation of these measures.

7. Accountability and Records of Processing

GDPR Article 5(2) requires WLIL to demonstrate compliance with the principles above, not merely assert it. WLIL maintains a data inventory and data flow record covering the business processes that use personal data, the source and volume of that data, its purpose, recipients, retention requirements, and any transfers, in line with Article 30's requirement to maintain a Record of Processing Activities (ROPA).

The small-organisation exemption from maintaining a ROPA (available to controllers with fewer than 250 employees under Article 30(5)) does not apply to WLIL, because that exemption is unavailable wherever processing includes special category data on anything other than an occasional basis — which describes WLIL's core activity. WLIL should treat its ROPA as a live compliance requirement, not an optional best-practice document.

7.1 Worked Example: Staff Location Monitoring via the Nourish Care Planner System

WLIL's Nourish Care Planner system (Nourish Empower) is used to log staff check-in and check-out at each service user's visit. For most visits, this check-in is app-based and records the location of the check-in; for certain clients, a one-time-password device is used instead. WLIL does not use landline check-in. This is included here as a worked example of a specific processing activity that must be captured in WLIL's Record of Processing Activities

under Section 7 above, since it involves collecting and linking location data to individual staff members — a distinct processing activity from ordinary visit or care record-keeping, and one that engages employee monitoring considerations, not only service user data protection.

For this processing activity specifically, WLIL should ensure:

- A documented legal basis is recorded for this specific processing — most likely legitimate interests (verifying that a visit took place as scheduled, supporting safe lone working, and supporting accurate payment of wages and travel expenses under WLILP50 - Travel and Subsistence Policy), balanced against the impact on staff privacy
- Staff are clearly informed that location data is collected as part of visit check-in, including in what circumstances it is used, who can access it, and for how long it is kept — this should not be left as something staff infer from using the app, and should be addressed directly in the Employee Handbook and at induction
- This processing is referenced in WLILP19 - Lone Working Policy, which describes the check-in methods in operational terms; this policy governs the data protection treatment
- Location data collected this way is retained in accordance with WLILP7D - Data Retention, Rectification and Erasure Policy, and is not repurposed for a use beyond what staff have been informed of, consistent with the purpose limitation principle at Section 6.2 above

8. Data Subjects' Rights

Individuals have the right to:

- make a subject access request to find out what data is held about them and why (see WLILP7C)
- have inaccurate data rectified, or incomplete data completed
- request erasure of their data in certain circumstances ("the right to be forgotten") (see WLILP7D)
- object to processing, including for direct marketing
- restrict processing in certain circumstances
- receive their data in a structured, commonly used, machine-readable format, and have it transmitted to another controller (data portability)
- not be subject to a decision based solely on automated processing, including profiling, which produces a legal or similarly significant effect on them
- lodge a complaint with the Data Protection Commission

9. International Data Transfers

Transferring personal data outside the European Economic Area (EEA) — referred to in GDPR as a "third country" transfer — is not permitted unless an appropriate safeguard applies:

- an adequacy decision by the European Commission, recognising that the destination country provides an adequate level of protection
- Standard Contractual Clauses (SCCs) approved by the European Commission, together with a Transfer Impact Assessment (TIA) confirming that the protection those clauses provide is not undermined by the law or practice of the destination country — the CJEU's Schrems II ruling (2020) made TIAs a required companion to SCCs, not an optional extra
- binding corporate rules, approved by the relevant supervisory authority, for transfers within a corporate group
- in the absence of the above, a specific derogation under Article 49 — for example explicit, informed consent from the data subject, or where the transfer is necessary for a contract with the data subject

This policy previously referred to the EU-US Privacy Shield as a valid safeguard for transfers to the United States. Privacy Shield was declared invalid by the Court of Justice of the EU in July 2020 (the "Schrems II" ruling) and has not existed since. Its replacement, the EU-US Data Privacy Framework (DPF), was adopted by the European Commission in July 2023 and remains in force at the time of writing — but it is itself under a live legal challenge: in July 2026, the privacy campaign group noyb (led by Max Schrems, whose earlier challenges struck down both the DPF's predecessors, Safe Harbor and Privacy Shield) called on the European Commission to begin an "orderly withdrawal" from the DPF, following a US Supreme Court ruling (Trump v. Slaughter, June 2026) that called into question the independence of the US oversight body the DPF relies on.

Given this history — two prior EU-US transfer frameworks have already been struck down by the courts — WLIL should not treat the DPF as a permanent fixture. Where WLIL relies on a US-based service provider, Standard Contractual Clauses with a Transfer Impact Assessment are the more resilient basis for the transfer, and WLIL should prefer a provider (such as its Microsoft 365 tenant, confirmed to store data in the North Europe/Dublin region — see WLILP29) that avoids the question of a third-country transfer altogether wherever practicable.

10. Data Protection Impact Assessments (DPIAs)

Where a type of processing, taking into account its nature, scope, context and purpose, is likely to result in a high risk to individuals' rights, WLIL will carry out a DPIA before that processing begins. A single DPIA may cover a set of similar processing operations presenting similar risks. Where a DPIA identifies that WLIL is about to begin processing that could cause damage or distress to data subjects, the decision on whether to proceed is escalated to the DPO, who will escalate to the Data Protection Commission if significant concerns remain.

11. CCTV and Visual Monitoring

WLIL operates CCTV at its office premises for the security of staff, visitors and property, and may rely on recorded footage as evidence in a disciplinary or grievance process. CCTV footage is personal data, and in some cases special category data (for example where it could reveal a health condition), so it is processed under this policy and the six principles in Section 6, not as a separate system outside GDPR.

- Purpose: CCTV is operated only for security and safety, and for investigating a specific incident or disciplinary/grievance matter. It is not used for continuous, routine monitoring of staff performance
- Signage: clear and visible signs are displayed wherever CCTV operates, naming WLIL as the data controller and how to make contact
- Access: recorded footage may only be viewed by the General Manager, the DPO, or another person specifically authorised by the General Manager for a named investigation. Access is logged
- Retention: footage is retained for no longer than necessary, and in any case no longer than the period set out in WLILP7D - Data Retention, Rectification and Erasure Policy, after which it is automatically overwritten or deleted
- Use in a disciplinary or grievance process: footage may only be relied on where it is relevant and necessary, and the employee concerned is told that footage is being relied upon and given the opportunity to view the relevant footage and respond, in line with WLILP55 - Disciplinary Policy and WLILP56 - Grievance Policy
- Data subject rights: a person recorded on CCTV may request a copy of their own footage under Section 8; footage of other identifiable people is redacted or blurred before release unless they consent
- DPIA: a Data Protection Impact Assessment is completed before any new camera is installed or the purpose of an existing camera changes, in line with Section 10

- No covert monitoring: WLIL does not use hidden or covert cameras except in the exceptional circumstances, and subject to the safeguards, set out in DPC guidance, and only with the General Manager and DPO's prior agreement

12. Disclosure and Security of Data

Personal data must not be disclosed to unauthorised third parties — including family members, friends, or government bodies — unless disclosure is relevant, necessary, and properly authorised by the DPO with supporting paperwork. All personal data should be accessible only to those who need it, in line with WLILP29 - Information Systems and Cloud Access Control Policy, and kept in a lockable office, locked drawer or cabinet, or password-protected system as appropriate. Manual records must not be removed from WLIL's premises without explicit written authorisation.

13. Training

All staff receive data protection training as part of induction, with periodic refresher training. Additional training is provided following any significant data protection incident.

14. Review

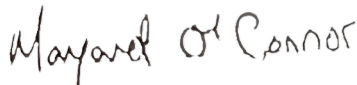
This policy, and WLILP7B, WLILP7C and WLILP7D, will be reviewed by the Board annually, or sooner if legislation, DPC guidance, or the status of the EU-US Data Privacy Framework changes.

This policy reflects GDPR, the Data Protection Act 2018, and current guidance on international transfers, checked as accurate as of drafting. It is not a substitute for legal advice; WLIL should have a solicitor confirm the DPO's independence from operational management, and should monitor the EU-US Data Privacy Framework's legal status given the active challenge described in Section 9.

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