

WEST LIMERICK INDEPENDENT LIVING CLG

Artificial Intelligence (AI) Use Policy

Policy Reference	WLILP71
Category	Operational Policies — Information Security and Data Protection
Version	1.0 (new policy)
Status	APPROVED — by the Board of Directors on 9 October 2026
Supersedes	None. This is a new policy. It extends WLILP29 (Section 8.5, secure use of Microsoft 365) and WLILP7A (Data Protection Policy) to cover artificial intelligence tools.
Policy Owner	Board of Directors, West Limerick Independent Living CLG
Applies To	All employees, Personal Assistants, contractors, consultants, temporary staff, trainees, volunteers and Board members who use AI tools for any WLIL purpose, on any device
Related Policies	WLILP7A - Data Protection Policy; WLILP7B - Data Breach Response Policy; WLILP29 - Information Systems and Cloud Access Control Policy; WLILP30 - Incident Management and Reporting Policy; WLILP45 - Training and Development Policy; WLILP47 - Confidentiality and Information Sharing Policy; WLILP52 - Induction Policy; WLILP55 - Disciplinary Policy; WLILP61 - Telephone Call Recording Policy; WLILP65 - Care Records and Documentation Policy
Review Cycle	Annually, or sooner if AI legislation, regulator guidance or the tools WLIL uses change

1. Purpose and Scope

Artificial intelligence (AI) tools can save time, but they can also expose personal information, produce wrong or biased answers, and tempt staff to hand decisions to a machine. This policy lets WLIL benefit from AI safely, and keeps people, not tools, responsible for decisions about service users and staff.

“AI tool” means any software that generates or analyses text, images, audio or video, or makes predictions or recommendations. This includes chatbots (such as ChatGPT, Microsoft Copilot or Gemini), AI features built into other software, AI note-takers and meeting or call transcribers, writing and translation assistants, and image, voice and video generators.

The policy applies to all use of AI for WLIL work, including on personal devices and personal accounts.

2. Legislative and Regulatory Framework

- **EU AI Act (Regulation (EU) 2024/1689)** — applies to WLIL as a “deployer” (an organisation that uses AI). Article 4 requires measures to support AI literacy among staff and others using AI on WLIL’s behalf. It has applied since 2 February 2025 and was reworded by the Digital Omnibus on AI (Regulation (EU) 2026/1744, in force from 27 July 2026), and national authorities enforce it from August 2026
- **Prohibited AI practices (Article 5)** — these include inferring people’s emotions in the workplace (other than for medical or safety reasons). WLIL does not use any prohibited practice
- **High-risk AI** — AI used for recruitment, managing workers, or deciding access to essential services is treated as “high-risk” under the Act, with obligations currently due to apply from 2 December 2027. WLIL’s position is not to use AI for these purposes (Section 7)

- **GDPR and the Data Protection Act 2018** — including data minimisation, lawful basis, special category (health) data, processor contracts (Article 28), data protection impact assessments (Article 35), breach notification (Article 33) and the right not to be subject to solely automated decisions (Article 22)
- **Data Protection Commission guidance, “AI, Large Language Models and Data Protection” (2024)** — organisations must assess whether an AI tool is necessary, understand how it uses the personal data entered into it, and put safeguards in place
- **Employment Equality Acts 1998–2015** — decisions about people must not be discriminatory, including through biased AI output
- **Draft National Standards for Home Support Services (2024) (HIQA)** — records and decisions about service users must be accurate and made by accountable people

3. Principles

- **People decide.** AI may assist, but a named member of staff is always responsible for the result and for any decision about a person
- **Protect personal data.** Personal information about service users, staff and others is not put into an AI tool unless that tool has been specifically approved for it
- **Check everything.** AI can be confidently wrong. Nothing is used until a person has checked it
- **Be honest and fair.** AI is not used to mislead, to impersonate, or to treat people unfairly
- **Use only approved tools.** Any tool not on the Approved AI Tools Register is not approved for use with personal or confidential information

4. Roles and Responsibilities

- **Board of Directors:** approves this policy, oversees AI risk, and reviews the policy annually
- **Manager:** approves or refuses AI tools and uses, maintains the Approved AI Tools Register, and ensures staff receive AI awareness training
- **Data Protection Officer (DPO):** advises on data protection risk, is consulted before any tool is approved for personal data, and advises whether a data protection impact assessment is needed (see WLILP7A)
- **IT lead** (the person or provider responsible for WLIL’s IT systems): checks security settings and access controls on approved tools (see WLILP29)
- **Coordinators:** make sure PAs and staff they supervise understand this policy and raise concerns
- **All staff:** follow this policy, complete AI awareness training and report any breach or concern immediately

5. Approving AI Tools

An AI tool may be used with personal or confidential information only if the General Manager has approved it, in writing, for a stated purpose and type of information, and has entered it in the Approved AI Tools Register (Appendix C). Approval for one purpose is not approval for another.

Before approving a tool, the General Manager, with the DPO and IT lead, completes the checklist in Appendix B. The key tests are:

- Is there a genuine need, and is there a simpler or safer way to do the same thing?
- Where is data processed and stored, and is it within the EU/EEA?

- Is there a written data processing agreement with the supplier, and does the supplier commit **not to use WLIL's inputs to train its models**?
- Can WLIL control who has access (individual work accounts with multi-factor authentication) and delete data on request?
- Has a data protection impact assessment been carried out where the tool will handle health or other special category data?

Free or personal accounts of public AI tools are **not approved** for any WLIL work involving personal or confidential information. A person's own device or account must not be used to get around this rule.

6. Personal and Confidential Information

The core rule is: **never enter personal or confidential information into an AI tool that has not been approved for that information.**

This includes names, initials used with other details, addresses and Eircodes, phone numbers, dates of birth, PPS numbers, bank details, photographs, voice recordings, and any information about a person's health, disability, care, behaviour, finances or family. It also includes safeguarding, complaint, grievance, disciplinary and investigation material, Board papers, passwords and security details.

Even in an approved tool, staff use the minimum information necessary and remove or replace identifying details wherever the task allows.

7. Permitted and Prohibited Uses

7.1 Permitted, with human checking

- Drafting or improving general documents that contain no personal information, such as templates, job advertisements, newsletters and policy drafts
- Summarising public or non-confidential material
- Formatting, spelling and grammar, spreadsheet formulas and brainstorming
- Converting non-personal text into plain language or easy-read format

7.2 Prohibited

- Using AI to **make or decide** anything about a person, including care needs, risk ratings, eligibility or referrals, recruitment shortlisting, performance, discipline or pay
- Using AI to write **care records, incident reports, safeguarding reports or SBAR forms** (WLILP30, WLILP65). These must be written by the member of staff who saw or did the thing recorded, from their own knowledge
- Using AI to infer or monitor the emotions, mood or behaviour of staff or service users, or to use facial recognition or biometric identification
- Creating or altering images, audio or video of any real service user or staff member, or impersonating any person
- Using an AI note-taker or transcriber to record calls, visits, meetings, supervision or assessments without prior written approval from the General Manager and the informed consent of everyone involved (see also WLILP61)
- Entering login details, security information or WLIL's systems configuration into any AI tool

- Presenting AI output as professional, clinical, legal or financial advice, or passing it off as checked when it has not been
- Using any AI tool in a way that bypasses WLIL's security controls

8. Accuracy and Human Oversight

AI tools can invent facts, sources, names and laws, and can reflect bias. The person using the output is responsible for it. Before anything produced with AI is used, sent or filed, the user must check the facts, figures, names and references against a reliable source, and must check that the wording is fair and appropriate. Where AI has materially contributed to a document going to the Board, the HSE or another funder, or the public, the author must be ready to say so if asked.

9. Transparency and Service User Rights

- If an approved AI tool processes a service user's or staff member's personal data, WLIL's privacy information (WLILP7A) must say so
- No service user or staff member is subject to a decision made solely by automated means that significantly affects them. A person is always involved and can be asked to review a decision
- Anyone can ask whether AI was used in connection with their information or a decision about them, and can object to it. Requests go to the General Manager and the DPO

10. Copyright and Confidentiality of Third-Party Material

Staff must not enter another organisation's confidential or copyrighted material (for example HSE documents, funder or contractor information, or commercial documents) into an AI tool without permission. AI output may reproduce copyrighted material, so it must not be published as WLIL's own without checking.

11. Incidents and Breaches

The following must be reported to the General Manager and the DPO **immediately**, and recorded under WLILP30:

- Personal or confidential information entered into an unapproved AI tool, or into an approved tool for an unapproved purpose
- AI output that contained a serious error, bias or harmful content, or that was used in a record or decision
- Loss or misuse of an AI account

The staff member must stop using the tool for that task and, where possible, delete the entry and chat history. The DPO decides whether the matter is a personal data breach. If it is, WLILP7B applies, including notification to the Data Protection Commission within 72 hours where required under Article 33 of GDPR.

12. AI Awareness and Training

WLIL will take measures to support the AI literacy of everyone who uses AI on its behalf, as Article 4 of the EU AI Act requires. This covers a short briefing at induction (WLILP52), an annual refresher through WLILP45, and role-based guidance for anyone who is approved to use AI tools with personal information. The General Manager keeps a record of who has been trained.

13. Monitoring and Non-Compliance

Use of WLIL's systems, including approved AI tools, is subject to the monitoring set out in WLILP29 (Section 9). WLIL does not monitor service users' personal activity. A deliberate or careless breach of this policy will be dealt with under WLILP55 - Disciplinary Policy.

14. Review and Updates

This policy is reviewed annually, or sooner if AI legislation, regulator guidance or the tools WLIL uses change significantly. The General Manager also reviews the Approved AI Tools Register at least once a year and removes tools that are no longer used or no longer meet the approval tests.

Legislative references and current guidance are checked as accurate as of this policy's drafting date (September 2026). AI regulation is changing quickly and dates and requirements should be re-checked at each review.

Appendix A — Quick Guide: Can I Use AI for This?

Task	Can I use AI?	Condition
Draft a general letter, template or newsletter with no personal details	Yes	Check the result before using it
Summarise a public report or website	Yes	Check key facts against the source
Improve wording, grammar or formatting of text with no personal details	Yes	You remain responsible for the final text
Write or tidy up a care note, incident report or safeguarding report	No	Must be written by the staff member who saw or did it
Paste in a service user's name, address, health or care information	No	Only in a tool the General Manager has approved for that information
Decide a risk rating, care need, referral, shortlist or performance outcome	No	Decisions about people are made by people
Record or transcribe a call, visit or meeting with an AI note-taker	No	Only with Manager approval and everyone's consent
Create an image, voice or video of a real person	No	Never permitted
Use a free ChatGPT or similar account for WLIL work with personal or confidential information	No	Not an approved tool
Not sure	Ask first	Ask your Coordinator or the General Manager before you use it

Appendix B — AI Tool Approval Checklist

Question	Answer / evidence
Tool name, supplier and version	
Purpose and business need. Is there a simpler or safer alternative?	

Question	Answer / evidence
What information will be entered? Does it include personal or special category (health) data?	
Where is data processed and stored? Is it within the EU/EEA?	
Is there a written data processing agreement (GDPR Article 28)?	
Does the supplier confirm it does not train its models on WLIL's inputs?	
Data retention, and how WLIL can delete data on request	
Access control: individual work accounts and multi-factor authentication (WLILP29)?	
Is a data protection impact assessment required? Completed?	
DPO consulted (name/date) and IT lead consulted (name/date)	
Decision, approved purposes and data types, conditions, and review date	

Appendix C — Approved AI Tools Register

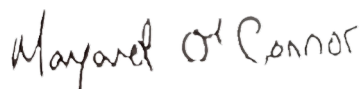
No AI tools are approved as of the date of this policy. The General Manager adds a tool here only after completing Appendix B.

Tool / supplier	Approved purpose	Information allowed	Conditions	Approved by / date	Review date

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:

