Willow Domestic Abuse Services

General Data Protection Policy

Version Date: January 2026

Version Control

Version Number	Author	Purpose/Change	Date
1.0	Ambit Compliance & Willow Domestic Abuse Services	Document creation	January 2021
2.0	Ambit Compliance & Willow Domestic Abuse Services	Review, rewording	10/12/2025
		Review Date	January 2026

Introduction

Willow Domestic Abuse Services is committed to ensuring the protection of personal data in compliance with the General Data Protection Regulation (GDPR) and the Data Protection Acts 1988-2018. This policy outlines our approach to lawful, fair, and transparent processing of personal data, ensuring all employees, contractors, and third parties adhere to applicable laws.

Scope

This policy applies to all personal data processed by Willow Domestic Abuse Services, including but not limited to employee, client, and third-party data. It applies to manual and automated processing activities, covering data collected, stored, shared, and disposed of by the organization.

Information relating to our processing of employee data can be found in our Employee Data Protection Policy.

All Personal and Sensitive Personal Data will be treated with equal care by Willow Domestic Abuse Services. Both categories will be equally referred-to as Personal Data

in this policy, unless specifically stated otherwise.

Data Controller/Data Processor Roles

Willow Domestic Abuse Services may act as:

- **Controller**: When determining the purpose and means of processing.
- **Processor**: When processing personal data on behalf of a third party.

Data Subjects

We collect data from a variety of data subjects. As part of our daily organisational activities, we process the personal data of prospective, current and former:

- Clients/Residents (this includes clients who engage with our helpline)
- Employees (see note below)
- Volunteers/Students
- Visitors
- Board directors
- Donors
- Business Contacts

Categories of Personal Data Processed

We may process the following personal data in relation to data subjects:

- **Clients** - Personal contact details e.g.name, address, gender, nationality, health info, contact number, email address, family/relationship status, partner and children's names and DOB, PPSN, current supports, health and safety incidents, meeting notes, CCTV images and footage.
- **Employees** – Refer to Employee Data Protection Policy for detail.
- **Suppliers** – name, employer, job title, bank details, correspondence
- **Website visitors** - IP address, click data.
- **Office visitors** - Time / Dates of attendance / Person visiting / CCTV images and Footage
- **Board members** – name, address, email, phone, DOB, other directorships, nationality, PPSN, training records, health and safety incidents, register of beneficial owners, register of directors, register of members.

We may also collect the following sensitive data:

- Health information
- Ethnicity

- Religion

Data Protection Principles

Willow Domestic Abuse Services is committed to processing data in accordance with its responsibilities under the GDPR. Article 5 of the GDPR requires that personal data shall be:

a. **Lawfulness, fairness, and transparency:** Personal data must be processed lawfully, fairly, and in a transparent manner.
b. **Purpose limitation:** Data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
c. **Data minimisation:** Only the data necessary for processing purposes will be collected and processed.
d. **Accuracy:** Personal data will be kept accurate and up to date.
e. **Storage limitation:** Data will be retained only for as long as necessary and securely deleted when no longer required.
f. **Integrity and confidentiality:** Appropriate security measures will be applied to ensure protection against unauthorised access, loss, or destruction.
g. **Accountability:** Willow Domestic Abuse Services will demonstrate compliance with data protection laws through documentation, policies, and internal controls.

Roles & Responsibilities

Willow Domestic Abuse Services Board: Provide oversight, set the tone, and ensure the organisation has the people, processes, and technology needed to protect personal data and comply with the law.

Data Protection Manager (DPM) (if applicable): Ensures compliance with GDPR and advises on data protection matters.

Senior Management: Oversees implementation and compliance with this policy.

Employees & Contractors: Must adhere to data protection policies and report any suspected data breaches.

Data Champions: Internal advocates who promote good use and protection of data in their part of the Willow Domestic Abuse Services. They help to turn policies into everyday practice and build a strong data culture.

Third-Party Processors: Must comply with contractual obligations ensuring GDPR compliance.

Legal Bases for Processing Personal Data

- **Consent**: Where permission/consent has been provided.
- **Contractual Necessity**: When processing is required to fulfil contractual obligations.
- **Legal Obligation**: When processing is required to comply with legal or regulatory requirements.
- **Legitimate Interests**: When processing is necessary for the legitimate interests of Willow Domestic Abuse Services or a third party, provided such interests are not overridden by data subject rights.

We process sensitive data based on one of the following conditions:

- Explicit consent of the data subject
- For the establishment, exercise or defence of legal claims
- For the purposes of preventative or occupational medicine; for medical diagnosis; for the provision of medical care, treatment or social care; for the management of health or social care systems as per Article 52 of the DPA 2018 (Ireland).

Individual Rights & Requests

Under GDPR, individuals have the following rights regarding their personal data:

- **Right to Access**: Obtain confirmation of data processing and access personal data.
- **Right to Rectification**: Request corrections to inaccurate or incomplete data.
- **Right to Erasure**: Request deletion of personal data under specific circumstances.
- **Right to Restrict Processing**: Request to limit processing in certain situations.
- **Right to Data Portability**: Receive data in a structured format and transfer it to another controller.
- **Right to Object**: Object to processing based on legitimate interests or direct marketing.
- **Rights related to Automated Decision-Making & Profiling**: Challenge automated decisions affecting them.

Requests to exercise these rights should be submitted to the Data Protection Manager or a designated contact point.

Data Collection, Use & Retention

Collection**:** Personal data will only be collected where necessary and through legal means.

Use**:** Data will be used strictly for the purposes stated at the time of collection.

Retention**:** Data will be retained in line with the Data Retention Policy, ensuring no longer than necessary storage periods.

Disposal**:** Secure deletion or destruction of data will be carried out when retention is no longer required.

Data Security & Breach Management

Security Measures: Willow Domestic Abuse Services implements technical and organisational measures to ensure personal data security, including encryption, access controls, and secure storage.

Incident Response: Any suspected data breach must be reported immediately. The organisation will assess the breach and notify the relevant supervisory authority within 72 hours if required.

Monitoring, IT & Marketing

Monitoring: Where monitoring (e.g. email, internet, or system usage) is necessary, it will be proportionate, justified, and communicated to individuals.

IT: Willow Domestic Abuse Services maintains robust IT security measures, including up-to-date antivirus protection, firewalls, access controls, and secure configurations. Updates are applied automatically, and devices are monitored for compliance.

Marketing: Any direct marketing activity will comply with the GDPR and the ePrivacy Regulations. Where required, consent will be obtained prior to sending marketing communications. An unsubscribe or opt-out mechanism will always be provided.

Training & Awareness

All employees handling personal data will receive regular training on data protection principles, policies, and best practices to ensure compliance.

Third-Party Data Sharing & Transfers

Third-Party Processors: Contracts will be in place to ensure compliance with GDPR obligations.

International Data Transfers: Any data transfers outside the EEA will be subject to

adequate safeguards, such as Standard Contractual Clauses (SCCs) or an adequacy decision.

Data Sharing

In terms of service users/residents who access the services and supports of the organisation, their data may be shared with professional agencies and organisations including statutory agencies, in the main with the consent of service users/residents through interagency working and this will be documented in the format of a consent form.

These agencies include the following:

Tusla Child and Family Agency, Meath County Council, Department of Social Protection, Department of Justice, Legal Aid Board and Legal Representatives, Local Authority Housing Departments, Gardai, Court Services, Adult Mental Health, GP's, Public Health Nurse, Schools, Therapeutic Services such as counselling, play and music therapists.

This list is not exhaustive and other relevant organisations may be contacted as the need arises.

In certain cases, we are legally obliged to share information on service users/residents e.g., in the case of a child protection referrals to Tusla as a mandated organization under the 2015 Children's Act.

In addition, anonymised Statistical information on our work which does not identify personal details of service users/residents is provided to our funders as part of our funding obligations and contract with funders e.g. Tusla, Victims of Crime. MOVE and other agencies who fund our work. etc.

The sharing of information will follow the principles of data protection, including its legal obligations.

Other Data Processors include providers of software we use to store and process data. These include:

- Sage
- Thesaurus
- ROS Online
- Microsoft Office 365

- Google
- PayPal
- I-donate.
- Stripe
- Tara Alarms or other-Management of Alarms and CCTV
- Evad and Enclude who manage our IT
- M1 Document Solutions shredding company.

Implementation

Failure of Willow Domestic Abuse Services staff to process Personal Data in compliance with this policy may result in disciplinary proceedings.

Transfers outside the EEA.

From time-to-time Willow Domestic Abuse Services may make use of services provided by 3rd parties which may necessitate the transfer of personal data outside of the EU/EEA. In these instances, we will choose providers who process data on the basis of:

- Model Contract Clauses
- An Adequacy Decision from the European Commission

If you Decide not to Provide Personal Data

We require certain information from you in order to deliver our service e.g., name and contact details. If you do not provide the personal data that we request from you it may hinder our ability to provide an effective support service to you.

Security

a. MWRSS shall ensure that personal data is stored securely using modern software that is kept-up to date.
b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorized sharing of information.
c. When personal data is deleted this should be done safely such that the data is irrecoverable.
d. Appropriate back-up and disaster recovery solutions shall be in place.

Data Breach

If there is ever a data breach including any loss, destruction, alteration or unauthorized disclosure of personal data, we will adhere to our Data Breach Policy and follow the steps outlined in our Data Breach Procedure.

CCTV

We use CCTV for the purpose of employee personal safety, business security and for the use in disciplinary investigations arising from alleged criminal activity or equivalent malpractice. These are deemed to be legitimate interests. Please refer to the CCTV Policy for further information.

Questions & Complaints

Questions about how your personal data is processed can be forwarded to the Data Protection Manager (See details in Appendix 1). Any complaints in connection to the processing of your personal data should also be forwarded to the Data Protection Manager.

As a data subject you also have the right to lodge a complaint with the Data Protection Commissioner if you are unhappy with our processing of your personal data. Details of how to lodge a complaint can be found on the Data Protection Commission's website (www.dataprotection.ie) or by phoning 1890 252 231.

Document Reviews

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

Appendix 1: Data Protection Manager Contact Details

Data Protection Manager

Name: Frances Haworth

Email frances.haworth@dvservicesmeath.ie

Phone 046 9022393

Appendix 2: Definitions

Organisation	Willow Domestic Abuse Services
Personal Data	Information which relates to a living individual, who can be identified either directly from that data, or indirectly in conjunction with other data which is likely to come into the legitimate possession of the Data Controller.
Sensitive Data	A particular category of Personal data, relating to: Racial or Ethnic Origin, Political Opinions, Religious, Ideological or Philosophical beliefs, Trade Union membership, Information relating to mental or physical health, information in relation to one's Sexual Orientation, Genetics or Biometrics.
Data Subject	A living individual who is the subject of the Personal Data, i.e., to whom the data relates either directly or indirectly.
Data Controller	A person or entity who, either alone or with others, controls the content and use of Personal Data by determining the purposes and means by which that Personal Data is processed.
Data Processor	A person or entity who processes Personal Data on behalf of a Data Controller on the basis of a formal, written contract, but who is not an employee of the Data Controller, processing such Data in the course of his/her employment.
GDPR	General Data Protection Regulation.
Responsible Person as Data Protection Manager	A person appointed by MWRSS to monitor compliance with the appropriate Data Protection legislation, to deal with Subject Access Requests, and to respond to Data Protection queries from staff members and service recipients.
Data Protection Champion	Supports the Data Protection Manager to monitor compliance with the appropriate Data Protection legislation, to deal with Subject Access Requests, and to respond to Data Protection queries from staff members and service recipients.