

Meath Women's Refuge and Support Services

General Data Protection Policy

Last updated	18 th January 2021
Review Date	January 2022

Definitions

Organisation	Meath Women's Refuge and Support 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	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

Protection Manager	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.

Purpose

The purpose of this document is to provide a concise policy statement regarding the Data Protection obligations of Meath Women’s Refuge and Support Services and to ensure that its data handlers understand the rules governing how they use the personal data to which they have access to during the course of their work.

This includes obligations in dealing with personal data, in order to ensure that the organisation complies with the requirements of the relevant Irish legislation, namely the General Data Protection Regulation (GDPR) and the relevant Irish legislation, namely the Data Protection Acts of 1988 – 2018.

Scope

The policy covers both personal and sensitive personal data held in relation to data subjects by MWRSS. The policy applies equally to personal data held in manual and automated form. 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 MWRSS. Both categories will be equally referred-to as Personal Data in this policy, unless specifically stated otherwise.

This policy should be read in conjunction with the associated Employee Data Protection Policy, Subject Access Request procedure, the Data Retention and Destruction Policy which includes Data Retention Periods and the Data Breach Notification procedure. MWRSS has also developed consent forms for women and children we work with.

Data Controller

Meath Women’s Refuge and Support Services (MWRSS) (referred to as ‘we’, ‘us’, ‘our’) is the Data Controller. Charity Number 8685, Company Number 127494. Our registered address is 39 Flower Hill, Navan, Co. Meath C15 HF72.

Data protection principles

MWRSS 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. processed lawfully, fairly and in a **transparent** manner.
- b. **Valid Purpose:** collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- a. **Data Minimisation:** adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. MWRSS shall only collect information required to complete its functions in terms of funding and legal requirements.
- c. **Accurate** and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- d. **Storage Limitation:** kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals. We will only store your data for as long as is necessary. For the purposes described here we will store your data in accordance with MWRSS Retention Schedule.
- e. **Secure:** processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.”

Responsibility

The Board has overall responsibility for ensuring MWRSS meets the requirements of the relevant legislation. The manager who acts the Data Protection Manager is responsible with the day-to-day adherence with policies and procedures. The Data Protection Manager and Data Protection Champion are responsible for rolling out data protection initiatives, reporting data protection issues and promoting a culture of privacy across the team.

This policy shall be reviewed by the board at least annually (January of each year).

Legal Basis of Processing

- a. All data processed by MWRSS will be done on one of the following lawful bases: consent, contract, legal obligation, public task or legitimate interests. MWRSS shall note

the appropriate lawful basis in the Register of Systems.

- b. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
- c. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent will be clearly available and systems will be in place to ensure such revocation is reflected accurately in MWRSS systems.

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)

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

The Personal Data We Collect

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

Why we collect Personal Data.

- ✓ To provide support services
- ✓ To make and take referrals.
- ✓ Responding to enquiries, complaints and feedback
- ✓ In line with our operational procedures e.g., training
- ✓ Respond to requests for data access, correction and other personal data rights.
- ✓ Comply with applicable laws and regulatory obligations e.g., tax, health and safety and legal obligations.
- ✓ Establish and defend legal rights to protect the business.

Third Parties with whom we share Personal Data.

As part of our role as Data Controller, we engage a number of Data Processors to assist in the smooth running of our business. This may involve processing of personal data. In each case, a formal, written contract is in place with the processor, outlining their data protection obligations, the specific purpose or purposes for which they are engaged, and the understanding that they will process the data in compliance with the Irish data protection legislation.

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, anonymized 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.
- Tara Alarms-Management of Alarms and CCTV
- Sentient Systems who manage our IT
- M1 Document Solutions shredding company.

Implementation

As a Data Controller, MWRSS ensures that any entity which processes Personal Data on its behalf (a Data Processor) does so in a manner compliant with the Data Protection legislation.

Failure of a Data Processor to manage MWRSS's data in a compliant manner will be viewed as a breach of contract and will be pursued through the courts.

Failure of MWRSS's staff to process Personal Data in compliance with this policy may result in disciplinary proceedings.

Transfers outside the EEA.

From time-to-time MWRSS 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.

Your Data Protection Rights

A data subject has various rights under data protection law, subject to certain exemptions, in connection with the processing of personal data.

- Right to access your data – the right to request a copy of the personal data that, together with other information about the processing of that personal data (Subject Access Request).
- Right to rectification – the right to request that inaccurate data is corrected, or incomplete information is completed.
- Right to erasure – the right to request the deletion of personal data.
- Right to restriction of processing or to object to processing – the right to request that personal data be no longer processed for a particular purpose, or to object to processing of personal data for particular purposes.
- Right to data portability - the right to request a copy of personal data be provided to the data subject or a third party in a structured, commonly used machine-readable format.

In order to exercise any of the above rights, please contact the Data Protection Manager in writing (see contact details in Appendix 1).

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. The CCTV scheme is controlled by MWRSS only. Access to recorded material is strictly limited to authorised personnel and is deleted every 30 days. 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: Sinead Smith

Email manager@dvservicesmeath.ie

Phone 046 9022393

Chairperson: Sinéad Gogan

Date: 18th January 2021