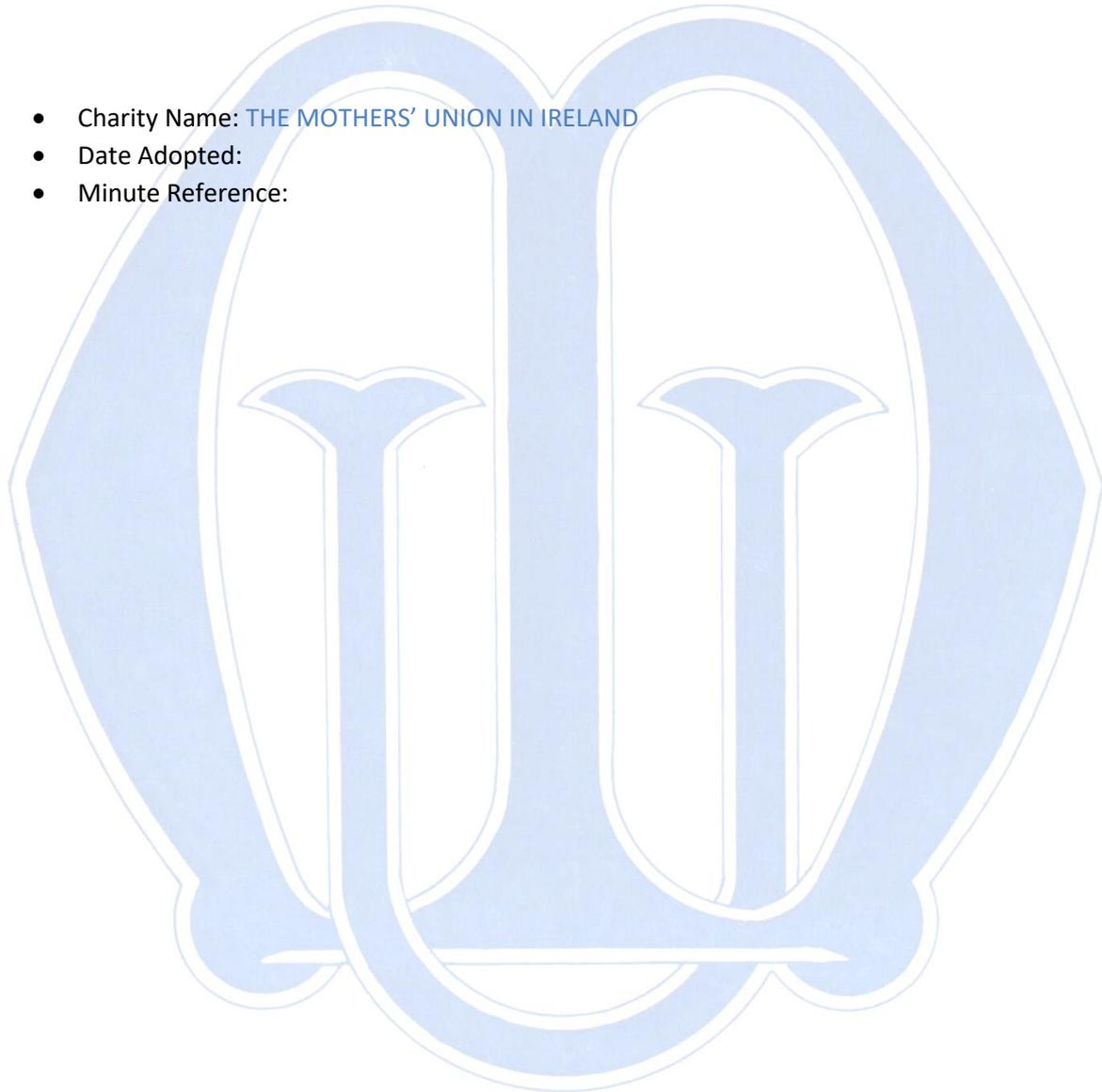

DATA PROTECTION POLICY

- Charity Name: THE MOTHERS' UNION IN IRELAND
- Date Adopted:
- Minute Reference:



Preamble

All members of the Board of The Mothers' Union in Ireland ("the Charity") are Charity Trustees within the meaning of the Charities Act 2009.

Introduction

This Policy sets out the obligations of the Charity regarding data protection and the rights of customers and suppliers ("data subjects") in respect of their personal data under the General Data Protection Regulation ("the Regulation").

The Regulation defines "personal data" as any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This Policy sets out the procedures that are to be followed when dealing with personal data. The procedures and principles set out herein must be followed at all times by the charity, its employees, volunteers, agents, contractors, or other parties working on behalf of the charity.

The charity is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals. If charities are not compliant, they can face a fine of up to 4% of their turnover or €20m, whichever is larger.

The Data Protection Principles

This Policy aims to ensure compliance with the Regulation. The Regulation sets out the following principles with which any party handling personal data must comply. All personal data must be:

- processed lawfully, fairly, and in a transparent manner in relation to the data subject;
- 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;
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods in so far 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 Regulation in order to safeguard the rights and freedoms of the data subject;

- 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

Data Processing by External Suppliers

It is the responsibility of the nominated 'Data Owner' (for each activity a person is logged as responsible for the handling of personal data) within the Dioceses to approve all subcontractors used by the Charity to process personal data on its behalf, according to the requirements of this procedure. It is the responsibility of the owners of third-party relationships to ensure that all data processing by third parties are carried out according to the requirements of this procedure. Regular audits of third-party compliance shall be carried out by the Data Owner, who shall be responsible for them.

Consent

Consent is defined as any indication on the part of the data subject that he or she agrees that their personal data may be processed. Consent must be given freely, without any duress, it must be specific, informed and without ambiguity and shall be granted by the data subject either by way of a statement or through clear, affirmative action on his or her part.

In relation to the processing of personal data of children under the age of 16, the Charity requires additional consent from the person who has parental responsibility over the child and the Charity must be able to demonstrate that this additional consent has been provided, as per a Parental Consent Form and that it has taken reasonable efforts to ensure that the claim of parental responsibility is authentic and true, including the use of available technology.

Retention Procedure

Role: Responsibility

President: To ensure that the collection, retention and destruction of all personal data by each department is carried out according to the requirements of the GDPR.

President: To ensure that all HR records are retained no longer than 6 years in total.

Administrator: To ensure that all Health and Safety records are retained in accordance to the Charity's Public Liability Insurance policy (normally 40 years).

Hon Treasurer: To ensure that all financial records, including accounting and tax records are retained for no longer than 7 years.

Hon Treasurer: To ensure that all relevant statutory and regulatory records are retained for statutory limitation periods (with the exception of the aforementioned records listed above).

Hon Treasurer: Donor's data if lapsed should not be kept beyond the 7 years tax audit.

Administrator: To ensure that all relevant statutory and regulatory records are retained (with the exception of the aforementioned records listed above).

Administrator: Consent to receive communication is advised to be refreshed every 2 years.

Data Breach

The Charity is required to provide the following to the supervisory authority in case of a data breach:

- A description of the nature of the personal data breach;
- The categories of personal data that have been affected by the breach;
- The number, which may be approximated if necessary, of data subjects affected by the breach;
- The number, which may be approximated if necessary, of personal data records affected by the breach;
- The name and contact details of the Data Owner (individual nominated within the Charity as responsible for the security of that data);
- The likely outcomes of the personal data breach;
- Any measures taken by the Charity to address and/or mitigate the breach; and
- All other information regarding the data breach.

General Training

The Charity is responsible for ensuring that all of its volunteers are aware of their personal responsibilities in relation to personal data, ensuring that it is properly protected at all times and is processed only in line with the Charity's procedures.

To this end, the Charity shall ensure that all of its volunteers are given appropriate and relevant training.

The Data Subjects Rights

- The right to access personal information;
- The right to withdraw consent;
- The right to amend personal data;
- The right to request that personal data be permanently deleted;
- The right to strict processing; and
- The right to raise an official complaint with the relevant authority;

Keeping Data Subjects Informed

The Charity shall ensure that the following information is provided - by reference to this Data Protection Policy - to every data subject when personal data is collected:

- Details of the Charity including, but not limited to, the identity of its Data Owner;
- The purpose(s) for which the personal data is being collected and will be processed and the legal basis justifying that collection and processing;
- Where applicable, the legitimate interests upon which the Charity is justifying its collection and processing of the personal data;
- Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
- Where the personal data is to be transferred to one or more third parties, details of those parties;

- Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the “EEA”), details of that transfer, including but not limited to the safeguards in place;
- Details of the length of time the personal data will be held by the Charity (or, where there is no predetermined period, details of how that length of time will be determined);
- Details of the data subject’s rights under the Regulation;
- Details of the data subject’s right to withdraw their consent to the Charity processing of their personal data at any time;
- Details of the data subject’s right to complain to the Office of the Data Protection Commissioner (the ‘supervisory authority’ under the Regulation);
- Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it;
- Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.

The information set out below shall be provided to the data subject.

Data Protection Measures

- The Charity shall ensure that all its employees, volunteers, agents, contractors, or other parties working on its behalf comply with the following when working with personal data:
- All emails containing personal data should be password protected and encrypted as attachments if the **diocese** is capable;
- Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hard copies should be shredded, and the more sensitive of personal data be securely shredded.
- Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances – if in doubt over the security of a network please seek the advice of the IT Manager at Mary Sumner House (ITManager@mothersunion.org);
- Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
- Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;
- Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient or postal service, preferably tracked;
- All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar;
- No personal data may be shared informally and if volunteer, agent, sub-contractor, or other party working on behalf of the Charity requires access to any personal data that they do not already have access to, such access should be formally requested from the Data Owner.

- No personal data may be transferred to volunteers, agents, contractors, or other parties, whether such parties are working on behalf of the Charity or not, without the authorisation of the Diocesan Hon Treasurer.
- Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, volunteers, agents, sub-contractors or other parties at any time.
- If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it.
- All personal data stored electronically should be encrypted and backed up.
- All electronic copies of personal data should be stored securely.
- All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords should contain a combination of uppercase and lowercase letters, numbers, and symbols.
- Under no circumstances should any passwords be written down or shared between volunteers, agents, contractors, or other parties working on behalf of the Charity, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords.

Organisational Measures

The Charity shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

- All volunteers, agents, contractors, or other parties working on behalf of the Charity shall be made fully aware of both their individual responsibilities and the Charity's responsibilities under the Regulation and under this Policy, and shall be provided with a copy of this Policy;
- Only volunteers, agents, sub-contractors, or other parties working on behalf of the Charity that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Charity;
- All volunteers, agents, contractors, or other parties working on behalf of the Charity handling personal data will be appropriately trained and supervised to do so;
- Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed;
- The performance of those volunteers, agents, contractors, or other parties working on behalf of the Charity handling personal data shall be regularly evaluated and reviewed;
- All volunteers, agents, contractors, or other parties working on behalf of the Charity handling personal data will be bound to do so in accordance with the principles of the Regulation and this Policy by contract;
- All volunteers, agents, contractors, or other parties working on behalf of the Charity handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees and volunteers of the Charity arising out of this Policy and the Regulation;

Implementation of Policy

This **updated** Policy shall be deemed effective as of **27 October 2021**. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

