
DATA PROTECTION POLICY

MISSIONARY SISTERS OF THE HOLY ROSARY



SEPTEMBER 2025

**MISSIONARY SISTERS OF THE HOLY ROSARY
GENERALATE HOUSE
KEADUE LANE
CAVAN
H12 YX53
Website: www.mshr.org
Charity Number: 3628**

Policy Management Information

Title	General Data Protection Regulation
Owner (Responsible)	Congregational Leadership Team
Author (Responsible)	GDPR Committee & GDPR Advisor
Version	1.0
Approved by	Congregational Leadership Team
Date of Approval	September 2025
Applicable to	Congregation Representatives including members of our Leadership Teams, Sisters of our Congregation, associated people (i.e. paid staff, volunteers, consultants, and visitors to our Communities and Ministries), in both their personal and professional lives
Frequency of Review	Every three years
Date of next review	September 2028
Related Policies & Procedures	Detailed within this Policy

Introduction

Everyone has rights with regard to how their personal data is handled. This Policy sets out the obligations of the Missionary Sisters of the Holy Rosary (hereafter MSHR) under data protection law and how that commitment is carried out with regards to the collection and use of personal data. Data protection law safeguards the privacy rights of individuals as well as laying down responsibilities for the processing of personal data. Data protection law imposes restrictions on how the MSHR may collect and process that data.

It is intended that by complying with these guidelines, the MSHR will adhere to best practice under data protection law.

Purpose

MSHR must comply with the data protection principles set out in the General Data Protection Regulation (GDPR)¹. The Policy sets out the rules and the legal conditions that must be satisfied in relation to the collecting, obtaining, handling, processing, storage, transportation and destruction of personal data.

Scope

The Policy applies to all personal data and sensitive data collected, processed and stored by MSHR in relation to its Sisters, employees, volunteers, benefactors and service providers in the course of its day-to-day activities.

Data can be held by MSHR in paper form or electronic form. The policy applies to all Sisters, members of staff including contractors and temporary personnel who process personal data as part of their work. MSHR treats the rights of all data subjects equally, whether they are Sisters, employees, volunteers or contractors.

Definition of Data Protection Terms

Data is information which is stored electronically on a computer or in paper files. This includes IT system and CCTV.

Data Subjects include all living persons about whom MSHR hold personal data

Personal data means data relating to a living person who is or can be identified either from the data or from the data in conjunction with other information that MSHR holds as a Data Controller. Personal data can be simple facts (such as a name, address or date of birth) or it can be opinion (such as a staff performance review)

Data Controller is the individual or organisation who controls and is responsible for the keeping and use of data. MSHR is a Data Controller

Data users include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following the Policy at all times.

Processing means doing anything with the data. There is a long list of examples of processing set out in GDPR. Some examples include collecting, recording or keeping data, using the data or destroying the data.

Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health, sexual life, criminal convictions or the alleged commission of an offence. Sensitive personal data can only be processed under strict conditions, and usually requires the consent of that person in order to process

Policy Objectives

MSHR processes personal data in the course of administering the Congregation, providing healthcare services to members of the congregation, fundraising from and engaging with benefactors, safeguarding, and engaging the services of employees and Charity trustees who are involved in providing those services.

Protecting the privacy of Data Subjects by ensuring and maintaining the security and confidentiality of personal and/or special category data is a compliance priority for MSHR.

Our data protection objectives are to:

- Ensure that individuals who entrust us with their personal data feel confident that their data will be handled in accordance with their rights under data protection laws;
- Ensure that all sisters, employees, volunteers and service providers involved in processing personal data are competent and knowledgeable about our data protection obligations and how they apply to their specific roles within MSHR;
- Enhance MSHR reputation as a reputable, trustworthy organisation which is committed to high standards of compliance and ethical behaviour;
- Minimise as far as possible the legal, financial or reputational risks to MSHR that can arise from processing personal data.

Data Protection Principles

MSHR Sisters and staff must deal with all personal data in a responsible manner and in accordance with the following eight data protection principles which state that data must be

1. Obtained and processed fairly
2. Used only for the purpose that it was gathered in the first instance
3. Kept safe and secure
4. Accurate and up to date
5. Disclosed only in line with the original purpose
6. Not excessive but relevant and adequate
7. Retained only for as long as needed for the original purpose
8. Presented to data subjects on request

Source: Data Protection Commissioner <https://www.dataprotection.ie>

Compliance with Major Principles

The principles of personal data management are described in GDPR.

Transparency, Purpose and Lawful Basis for Processing

MSHR advises all Data Subjects about what data it collects, what it is used for, who it might be shared with, where and for how long it may be retained, and how it is secured in addition to other relevant details about processing personal data. We also advise data subjects of their rights, where to get further information and how to make a complaint.

MSHR establishes the purpose and lawful basis for processing before processing any personal data and these are set out in our Privacy Notice.

Purpose Limitation

MSHR processes personal data only for the stated purpose or for purposes that are compatible with the original purpose. If processing for an incompatible process is contemplated, we will seek the consent of the Data Subject before processing the data for the new purpose.

Data Minimisation

MSHR only ever obtains, retains, processes, and shares the minimum amount of personal data that is essential for carrying on our business and/or meeting our legal obligations.

Accuracy and Quality

MSHR takes steps to ensure the accuracy and quality of personal data processed and acts to rectify any inaccuracies where they occur.

Retention and Storage Limitation

MSHR retains and stores personal data only for as long as is necessary for the purpose for which the data is processed and deletes or disposes of it securely when it is no longer required. In addition to retaining personal data for the administration of the Congregation and its services. MSHR also maintains an archive which includes certain personal data, which is considered to be of enduring historical value and public importance.

Security and Confidentiality

MSHR has adequate and appropriate technical and organisational measures commensurate with the risk to the Data Subjects to ensure the security, and maintain the confidentiality, of personal data processed.

How are the Data Protection Principles applied at MSHR?

In the course of its daily organisational activities, MSHR acquires, controls, processes and stores personal data of data subjects.

Data protection law imposes restrictions on how MSHR may collect and process that data.

When gathering personal data MSHR must state its reasons for looking for it, what it will be used for and who it will be shared with. MSHR must ensure that any data collected is limited to what it actually needs, for purposes which are specific, lawful and clearly stated.

Before MSHR process any personal data it must tell data subjects that they have a right to complain if they are unhappy with the reasons for processing and what rights they have under GDPR. MSHR must ensure that it uses technical measures and has procedures in place to secure the personal data against unauthorised access, unlawful process or accidental loss or damage.

Where possible MSHR will seek the consent of the data subject before their data is processed. Where it is not possible to seek consent, MSHR will ensure that collection of the data is

justified under one of the other lawful processing conditions set out under GDPR, for example, legal obligations for a contract etc.

MSHR, as an employer, collects personal data of its staff to create an employment contract. MSHR processes the personal data of staff in order to pay wages, and maintain a personnel file etc.

Access to and management of staff is limited to those staff members who have appropriate authorisation.

Benefactors

MSHR must also comply with statutory obligations and under some laws MSHR can be obliged to share personal data of data subjects, for example, to An Garda Síochána where a crime has been committed.

Where MSHR intends to record activity on CCTV, a notice will be posted in full view. For further details on the use of CCTV, see MSHR's CCTV policy.

If a person visits MSHR website to browse, read or download information MSHR automatically collects and stores information about the use of the website through certain cookies that are set. Please refer to MSHR's Cookies Policy and Privacy Policy.

This can be found on the website at www.mshr.ie/privacy-policy.

What obligations must MSHR Sisters and staff members comply with?

Keep Confidential

All MSHR Sisters and staff must keep confidential any personal data they are using as part of their work or employment. Not all Sisters and staff members are expected to be experts in data protection law. However, MSHR is committed to ensuring that its Sisters and staff are sufficiently aware of the data protection law in order to be able to anticipate and identify a data protection issue, should one arise.

Mandatory Training

MSHR has provided data protection awareness training to all Sisters and staff members which provides them with the ability to recognise, report and address potential data breaches and to respond to subject access requests efficiently. Sisters and staff have been trained to ensure that where personal data must be shared with suppliers that MSHR will only use suppliers who have robust data protection policies in place (See **Third Party Processors** below).

Keep Data accurate

MSHR is obliged to keep personal data accurate and up to date. MSHR must correct information which is inaccurate or misleading. MSHR must take steps to check the accuracy of any personal data when it is being collected and at regular intervals afterwards. Inaccurate or out of date data should be destroyed.

Notify of changes

Sisters and staff members should ensure that they notify their manager/Human Resources of any relevant changes to their personal information so that it can be updated and maintained accurately, for example, a change of address.

Keep for only as long as necessary

Personal data should not be kept longer than is necessary for the purpose for which we collected it. For guidance in relation to data retention policies staff members should contact their manager. This means that the retention period for personal data will vary depending on the type of personal data and the reason it was collected. MSHR has various regulatory and legal obligations to keep certain data for a specified period of time. MSHR will conduct regular assessments in order to establish the need to keep certain personal data. Where it is no longer required to be kept, MSHR will destroy, erase or otherwise put this data beyond use.

How can Sisters and Staff Members ensure that data is kept safe?

Sisters and Staff members must ensure that data is kept safe by:

1. Ensuring desks and cupboards are kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
2. When destroying information, paper documents should be shredded. Floppy disks and CD-ROMs should be physically destroyed when they are no longer required.
3. Data users should ensure that individual monitors do not show confidential information to passers-by and that they lock or log off from their PC when it is left unattended.

Providing information over the phone

Any Sister or staff member dealing with telephone enquiries should be careful about disclosing any personal data held by MSHR over the phone. In particular, the sister/staff member should:

1. Check the identity of the caller to ensure that information is only given to a person who is entitled to that information.
2. Suggest that the caller put their request in writing if the Sister/staff member is not sure about the identity of the caller, and in circumstances where the identity of the caller cannot be verified.
3. Refer the request to their manager for assistance in difficult situations. No Sister/staff member should feel forced into disclosing personal information.

How does MSHR manage personal data queries?

MSHR has set up a Data Protection Working Group (“DPWG”) to handle and respond to all personal data queries. The DPWG is led by the Data Protection Representative who is also responsible for monitoring and continually improving internal data protection processes. The Data Protection Representative can be contacted by telephone: +353 49 389 1511 or by emailing dataprotection@mshr.ie

Subject Access Requests

All individuals who are the subject of personal data held by MSHR are entitled to:

- Ask **what information** the organisation holds about them and why.
- Ask **how to gain access** to it.
- Be informed about **how to keep it up to date**.
- Be informed about how the organisation is **meeting its data protection obligations**.

Should an Individual contact the organisation requesting this information, this is called a Subject Access Request (SAR).

Subject Access Requests from individuals should be made by email, addressed to the data controller at mshrgen@eircom.ie. The data controller can supply a standard request form, although individuals do not have to use this.

The data controller will aim to provide the relevant data within **30 days**.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Consent

MSHR understands ‘consent’ to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject’s wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.

MSHR understands ‘consent’ to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the grounds of misleading information will not be a valid basis for processing.

There must be some active communication between the parties to demonstrate “active consent”. Consent cannot be inferred from non-responsive communications. The controller must be able to demonstrate that consent was obtained for the processing operation.

For sensitive data, explicit consent from data subjects must be obtained unless an alternative legitimate basis for processing exists.

Retention and Disposal of Data

MSHR shall not keep personal data in a form that permits identification of data subjects for a longer period than is necessary, in relation to the purpose(s) for which the data was originally collected.

MSHR may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or

statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

The retention period for each category of personal data will be set out in the Retention of Records Procedure, along with the criteria used to determine this period, including any statutory obligations MSHR has to retain the data.

MSHR Data Retention, Data Disposal and Storage Removal Procedures will apply in all cases.

Personal data must be disposed of securely, in accordance with the sixth principle of the GDPR. Thus, processed in an appropriate manner to maintain security, thereby protecting the “rights and freedoms” of data subjects. Any disposal of data will be done in accordance with the Secure Disposal Procedure.

Third Party Processors

As MSHR controls and is responsible for keeping and using personal data on its computers or in manual files, it is known as a Data Controller. This means MSHR has obligations under data protection law to keep the data safe. As part of its day-to-day business activities, MSHR engages trusted third parties to carry out work on its behalf. Some of these third parties must hold or process the personal data to perform their job. These third parties are known as Data Processors. To ensure that all personal data that is held or processed by Data Processors is kept safe, a written agreement is entered into with the Data Processor, which sets out their obligations to MSHR. It sets out the specific purpose or purposes for which they are engaged, and the understanding that they will process the personal data in compliance with data protection law.

Data Breaches

It is important that all Sisters and staff are aware whom they should report such a breach. Sisters and staff need to be made fully aware as to what constitutes a data breach. MSHR has a Data Breach Policy in place and this forms part of the Sisters and staff awareness training. Having such a procedure in place will allow Sisters/staff to recognise a breach or a potential breach early on so that it can be dealt with in the most appropriate manner.

Details of a data breach should be recorded accurately, including the date and time the breach occurred, the date and time it was detected, who/what reported the breach, description of the breach. For further information, see the Data Breach Policy.

Photos/Video

The use of photos/videos on websites and in other online/hard copy publications can pose direct and indirect risks to all and specifically children and vulnerable adults. It is important that all follow the correct procedures when taking and using photos/videos. Where applicable, comply with local data protection laws.

Phone numbers:

Phone numbers are considered Personal Data in most Data protection Law in Europe. That means you can't just share someone's number freely.

When you should not share someone's number

-you don't have their consent

- the number is being shared for other purposes than it was originally given
- sharing it could harm their privacy or reputation.

When you can share a phone number

- You have clear consent from the person
- in some emergency where safety is at risk.
- If the number is publicly advertised for business, etc

Enforcement

The policy applies to all Sisters/staff and volunteers of MSHR. It also applies to contractors and temporary personnel of MSHR.

Adherence to the Policy is overseen by the managers. If a sister/employee/volunteer considers that the Policy has not been followed in respect of personal data about themselves or others they should raise the matter with their manager as soon as possible.

The Data Protection Representative will monitor any breaches of the Policy and will work in tandem with the manager to ensure ongoing general compliance. Data protection training will be continually offered to the Sisters and staff. Any breach of the Policy will be taken seriously and depending on the severity and nature of the breach may result in disciplinary action up to including dismissal. MSHR reserves the right to take such action as it deems appropriate against any data users who breach the conditions of this policy.

Roles and Responsibilities

Trustees/Leadership	Approve the Data Protection Policy and oversee implementation of good data protection management practices Allocate responsibilities and provide sufficient resources. Lead by example: make data protection a priority and incorporate it into management systems and processes.
Data Protection Representative	Responsible for compliance with data protection legal requirements and championing good data protection practices in SPMS Ireland.
Department Managers	Responsible for complying with this policy and complying with data protection procedures and guidance in respect of the personal data processed by their department.
Sisters/Employees/Volunteers	All are responsible for familiarising themselves with the policy and ensuring that any data that they handle is processed in accordance with this policy and related procedures. They have a role to play in ensuring that personal data that they use in their work is kept secure and confidential. Sisters/employees/volunteers are responsible for reporting any potential breach or loss of personal data for which they are responsible or become aware of to their line manager.

MSHR is a (Data Controller under the GDPR)

Leadership and all those in managerial or supervisory roles throughout MSHR are responsible for developing and encouraging good information handling practices within MSHR; responsibilities are set out in individual job descriptions.

GDPR Representative

The organisation made a decision not to appoint a Data Protection Officer but has appointed a representative with responsibility for GDPR.

Sr. Ruth Chetambe is the appointed person for GDPR and can be contacted via:

Phone: +353 49 389 1511

Email -cltdevelopment@mshr.org

The GDPR Representative's specific responsibilities are in respect of procedures such as the Subject Access Request Procedure and are the first point of call for Sisters/Employees/Volunteers, seeking clarification on any aspect of data protection compliance.

Compliance with data protection legislation is the responsibility of all Sisters/Employees/Volunteers who process personal data.

MSHR Training Policy sets out specific training and awareness requirements in relation to specific roles and Sisters/Employees/Volunteers.

Sisters/Employees/Volunteers of MSHR are responsible for ensuring that any personal data about them and supplied by them to MSHR is accurate and up-to-date.

Everyone who works for or with MSHR has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

The **Generalate** is ultimately responsible for ensuring that the MSHR meets its legal obligations.

The **GDPR Representative Person**, is responsible for:

- Keeping the Generalate updated about data protection responsibilities, risks and issues;
- Reviewing all data protection procedures and related policies, in line with an agreed schedule;
- Arranging data protection training and advice for the people covered by this policy
- Handling data protection questions from Sister/employees/volunteers and anyone else covered by this policy
- Working with the Data Protection Working Group to deal with requests from individuals to see the data the MSHR holds about them (also called Subject Access Requests)
- Checking and approving any contracts or agreements with third parties that may handle the organisation's sensitive data.
-

Review of Policy

MSHR will continue to review the effectiveness of the Policy to ensure it is achieving its stated objectives on at least an annual basis and more frequently if required taking into account changes in the law and organisational or security changes.

Data Protection Principles

The ***General Data Protection Regulation (GDPR) (EU)2016/679*** was approved by the European Commission in April 2016 and applies in all EU Member States from 25th May 2018. As a '*Regulation*' rather than a '*Directive*', its rules apply directly to Member States, replacing their existing local data protection laws and repealing and replacing Directive 95/46EC and its Member State implementing legislation.

As MSHR processes personal information regarding individuals (*data subjects*), we are required under the General Data Protection Regulation (GDPR) to protect such information, and to obtain, use, process, store and destroy it, only in compliance with its rules and principles. MSHR has additional responsibilities under the Data Protection Acts 1988-2018 and (If applicable the UK Data Protection Act 2018).

Article 5 of the GDPR requires that personal data shall be: -

- a) Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')
- b) 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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
- d) 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 ('accuracy')
- e) 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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')
- f) 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 ('integrity and confidentiality').

Article 5(2) requires that 'the controller shall be responsible for, and be able to demonstrate, compliance with the data protection principles (**'accountability'**) and requires that organisations **show how** they comply with the principles, detailing and summarising the measures and controls that they have in place to protect personal information and mitigate the risks of processing.

References

For further information relating to data protection please refer to:

- Privacy Notice
- Retention Policy
- Data Protection Commissioner's Website <https://www.dataprotection.ie>

Forms

Subject Access Request (SAR)

Privacy Notice

This Privacy Notice gives you some helpful information about who we are, what personal data we collect about you, why, who we share it with and why, how long we keep it, and your rights.

Who we are:

We are the Missionary Sisters of the Holy Rosary Generalate, Killeshandra House, Keadue Lane, Co. Cavan., Ireland (hereafter known as MSHR). We are totally committed to protecting the rights and privacy of every individual. We are aware of the GDPR Regulations that came into effect across Europe on 25th May 2018 and committed to the basic principles of the GDPR regulations.

What personal data we collect and why

We collect and use personal data relating to our Sisters, our employees, and others with whom we engage.

Sisters' Personal information

We collect and process personal data of Sisters (including former members and applicants). This personal data includes: The name; date of birth; address and contact details; CV, education and qualifications; religion; data relating to training, formation, discernment, and vocation; canonical processes; Vetting data and Safeguarding data; PPS number; financial data; photos/images (including for CCTV); pensions and/or benefit entitlements; medical, health and occupational health data; immigration/work-visa information; information relating to recruitment, promotions, appointments processes, retirement details, next-of-kin. We

process this data for compliance with our Legal Obligations and for the legitimate activities of a not-for profit religious body.

Family information

We hold the addresses and contact details of Sisters' family members, so that we can contact them in case of an emergency, and let them know about Cemetery Days and/or other events. We process this data in compliance with our legal obligations and for the legitimate activities of a not-for-profit religious body.

Archives

Sisters' data are transferred to the Congregation's archives, held by the MSHR being the body having responsibility for the Congregational archives. This processing is based on the lawful basis of our legitimate activities of a not-for-profit religious body, for substantial public interests and for the establishment, exercise or defence of legal claims.

Sisters provide personal data to the Charity in order for the Charity to comply with canon law and civil law requirements

Photographs

We take photographs and films ("images") of our Sisters for use on our website and social media account. We use these images taken at Congregational events (e.g. Jubilee celebrations, community events, etc.) for the purpose of maintaining a visual record of the Sisters and the vibrant life of our Congregation. If a person attends an event at which we are taking photographs we will ask for their Consent to take and use the photographs. We may display these photographs in Congregational properties and use them in Congregational literature. If Consent is given to put the photographs up on our social media page the photographs will also be subject to the privacy policy of the social media site. Consent can be withdrawn at any stage, and we will remove the photograph from our website according to the person's preferences.

Employees

We collect and process personal data of employees and those applying for jobs. The personal data we collect includes: the person's name; date of birth; address; contact number or email. We process this data for the performance of a contract or to take steps prior to entering into a contract, namely the employment contract.

For employment data and pre-employment checks we request CVs with details of education, experience and qualifications; Vetting data and Safeguarding data; registration with any other professional regulatory and/or accrediting body; PPS number; financial data. We process this data for the following purposes: for the performance of a contract or to take steps prior to entering into a contract, namely the employment contract; due to a legal obligation; for the purposes of carrying out the legal obligations of the controller in the field of employment law.

Benefactors

We collect and process personal data of benefactors who make charitable donations to us. This personal data includes your name, address, email address, phone number, and details of when you were last in contact with us.

We will use your personal data for the following purposes:

- **To process donations:** If you make a charitable donation, we may collect your financial information (e.g. credit or debit card details) for the purposes of processing your donation. We will use your personal data to send you a receipt and thanks for any donation (by email or SMS text message if you have provided us with those details for those purposes). We process this personal data on the basis of your
- **Consent.** We will not use your email address or mobile phone number for any other purpose other than acknowledging your donation. If you wish to enable us to claim back the tax on your donation from the Revenue Commissioners, and you complete a Forum CHY3 or CHY4 for that purpose, the form will contain your PPS number and will be submitted to the Revenue Commissioners for the Charity to recover the tax back on your donation. If you establish a standing order for your charitable donation, we will hold your bank account details and payment instruction only until the standing order is set up.
- **To send you communications, news, appeals materials:** If you give us your Consent to doing so, we will write to you (usually by post) to tell you about our charitable projects and fundraising activities, to send you calendars or other seasonal materials. If at any time you no longer wish to receive these from us, you can opt-out of receiving those letters at any time by contacting us.
- **Administering bequests:** where a benefactor leaves us a bequest in their Will, we retain the Will (and correspondence with the estate's solicitors) to administer the donation and comply with financial audit requirements as a registered charity, to remember the benefactor and their family in Masses, and (where appropriate) communicate with their next of kin or executor to express our thanks for the bequest.
- **Photographs:** If you attend an event at which we are taking photographs to put up on our website or social media page (e.g. Facebook) we will ask for your Consent to take your photograph and put it up on the website and social media page. If you give your Consent to this use, the photograph will be subject to the privacy policy of the social media site. You can withdraw your Consent at any stage, and we will remove the photograph from the social media page and/or website according to your preferences.

How long we keep it

The Charity complies with the storage limitation principle by only keeping data for the period necessary for the purposes for which the data are processed. How long we retain personal data depends on various factors. Some personal data is only kept for a short period. For example, a completed CHY4 Annual Certificate is required in the "active" accounting system for the current tax year until the Revenue Commissioners have refunded the tax to the charity. Then they are retained for audit purposes and any audit by the Revenue Commissioners (usually 6 years after the end of the audit to which they relate). Some data we retain for a longer period (e.g. if you are an employee of the Charity, we retain your data after you leave or otherwise finish your employment with us, for example where same are required for

employment references, or pension purposes etc). Some data we retain indefinitely due to its enduring historical value (e.g. information that will have enduring historical value for archival purposes). If a benefactor remembers us in their Will, we will keep the Will (and any correspondence with the estate) in our active accounting system for accounting and audit purposes in line with our legal obligations as a registered charity; after that, we transfer the Will to our Congregational archives which are held by MSHR. We believe that benefactors' Wills are documents of enduring historical value and we retain that to honour the testator's memory and to acknowledge the meaningful contribution they have made to the work of the Congregation.

The Congregational archives are not open to the public. We will retain personal data to manage risk, to prevent fraud, for insurance purposes, to resolve disputes and take or defend litigation etc.

If you would like further information about retention periods, please contact us.

Who we share with

We share personal data with third parties where required to comply with our legal obligations (including complying with court orders, discovery orders, etc.). Where required, we will share your personal data with our insurance company, our legal advisors, and other service providers (including auditors, payroll providers, IT providers, security providers, etc.) to enforce our legal rights (for fraud prevention, credit risk, litigation) and to resolve disputes and defend litigation.

- **Benefactors:** we share your personal data with parties including the Revenue Commissioners (to claim the tax-back on any charitable donations, where applicable), with payment service providers (such as PayPal to process the credit/debit card transaction on any subscription or donation), with our banks (to process any cheques etc.). After completion of the payment, the documentation is retained and shared with our Auditors for audit and verification purposes (in compliance with our financial audit requirements as a registered charity). Our financial records and donations information can be audited by the Charities Section of the Revenue Commissioners and/or the Charities Regulatory Authority for regulatory compliance. After completion of the payment, the documentation is retained and shared with our Auditors for audit and verification purposes (in compliance with our financial audit requirements as a registered charity). Our financial records and donations information are disclosed to the Charities Section of the Revenue Commissioners and/or the Charities Regulatory Authority in any audits and/or investigations. If consent is given to use photographs, the photograph is subject to the privacy policy of that social media company. Where necessary for security, fraud-prevention, cyber-security, and where same is in our legitimate interests, we will report relevant matters to and share data with An Garda Síochána and other police and law enforcement authorities.
- **Sisters:** we share Sisters' personal data with Colleges/educational institutions which our members are attending as part of training, formation, discernment, vocations, sabbaticals, etc.; other Regions and the Generalate Team; with Dioceses and parishes in Ireland and the UK. In respect of any safeguarding information relating to members, we share data with TUSLA, An Garda Síochána, medical professionals and clinical bodies, and other Church bodies. If a Sister is in a care facility, the personal data will be shared with the Sister's GP, Doctors, clinical care team (including

occupational therapists, speech therapists, physical therapists), other Hospitals and care facilities, the HSE, and with other bodies who may be in a position to assist in meeting the person's care needs. We may also share their personal data with their close family/next-of-kin if the person consents or requires us to do so, or in case of an emergency. Sisters' data may be disclosed to the Charity's auditors in compliance with our financial audit requirements as a registered charity.

- **Employees:** we share employees' data with third parties, including other Government bodies including Revenue Commissioners, Department of Social Protection, TUSLA, An Garda Síochána, and the HSE; any regulatory body to which the employee belongs; your Trade Union (for employment rights, IR/HR issues etc.); occupational health advisors and registered medical professionals; our insurance company (re any claims and/or insurable events); banks/financial institutions (to pay wages); pension administrators and pension trustees (re the occupational pension scheme); future employers (if the employee requires an employment reference, etc.); other service providers (including IT providers, security providers, legal advisors), etc. The Government bodies to which we transfer your personal data will use it for their own purposes (including: to verify other information they already hold about you, for fraud prevention measures, etc.) and may aggregate it with other information they already hold about you.

If you would like further information about who we share your data with, please contact us.

Website

We have a website at www.mshr.org. If a person chooses to provide personal data via this website (e.g. name, email address, message) we will use that information to contact the person and/or respond to the query where relevant.

General Charity records

We use personal data based on our legitimate interests. The legitimate interests are our charitable objectives, and to run an efficient charity.

Legitimate interests, legitimate activities, and substantial public interests

We use personal data for purposes including: running the body in compliance with our canon law obligations; allocating resources across our organisation; complying with all our legal obligations (in canon and civil law); complying with our obligations as a charitable body; to work in partnership with other Church bodies (e.g. local parishes, National Board for Safeguarding Children in the Catholic Church in Ireland etc.); to discharge our duties to our Sisters and to others; complying with our obligations to Government bodies; to manage risk; for resolving disputes and taking/defending litigation etc. We process this data in compliance with our legal obligations and for the legitimate activities of a not-for-profit religious body, for substantial public interests and for the establishment, exercise or defence of legal claims.

Employees have to provide the Charity with such information as is relevant to their employment, otherwise the Charity cannot comply with its legal obligations as an employer.

to the Charity's auditors in compliance with our financial audit requirements as a registered charity.

Third Country Transfers

In general, the Charity does not transfer personal data outside the EEA. However, transfers to third countries can arise with Sisters' personal data in some limited situations. For example, where a Sister is being sent to the missions, we send her data to the Sisters in community in that jurisdiction in preparation for her arrival.

Your rights

You have the following statutory rights that can be exercised at any time subject to the limitations and exceptions set out in GDPR and the Data Protection Act 2018. You can exercise these by contacting us, and providing us with proof of identity and the detail of your request:

Rights

- Right of access.
- Right to rectification.
- Right to erasure (right to be forgotten).
- Right to restrict processing.
- Right to data portability.
- Right to object.
- Right not to be subjected to automated decision making/profiling.

Contact us

If you have any queries, please contact us at:

Missionary Sisters of the Holy Rosary Generalate

Killeshandra House

keadue lane

Cavan

H12 YX53

website: www.mshr.org

charity number: 3628

Data Protection Subject Access Request (SAR) Application Form

Request for access to Personal Data under the General Data Protection Regulation (GDPR) and Data Protection Acts 1988-2018.

Notes:

- 1. In order to respond to your request for personal data, you will need to provide us with adequate Proof of Identity.*
- 2. Where a request is manifestly unfounded, excessive, of a repetitive nature or where more than one copy of the data is sought, a fee may apply.*
- 3. You may contact our Data Protection Representative to assist you in the completion of this Form.*
- 4. A copy of our Privacy Notice is available at: Secretariate*

Data Retention

We will only keep a copy of these documents until your subject access request has been fully processed and issued to you and all relevant review or appeal procedure timelines have expired.

Please complete **all** parts of this form in **full**.

Part 1 – Details of Data Subject (Your Details)

Contact Details (in block capitals):

Name:

Surname:

Address:

Eircode:

Contact Phone Number:

E-mail Address (where applicable)

Part 2 – Details of Request

Help Us to Help You!

To assist us in locating the data you are requesting, please include as many specific details as possible in relation to your interactions with us in the past (e.g. please state the area(s) of the Office you have corresponded with/the types of applications you may have made, etc).

Please tell us the relevant period of time or timelines involved (i.e. the relevant dates e.g. *01 January 2019 – 31 December 2019* for which you are seeking the personal data).

Please provide us with any reference numbers relating to your contact with us in the past (e.g. previous correspondence references, case reference numbers, etc.).

Please provide us with any other specific details that you feel are relevant in assisting us in locating your personal data. (e.g. by providing us with as much detail as possible in relation to your access request, we will be able to assist you more efficiently).

Part 3 – Declaration

I declare that all the details I have provided in this Form are true and complete to the best of my knowledge.

Signature of Requester: _____

Date: _____

Please return the completed Form by post to:

Data Protection Representative

MISSIONARY SISTERS OF THE HOLY ROSARY GENERALATE

KILLESHANDRA HOUSE

KEADUE LANE

CAVAN

H12 YX53

Website: www.mshr.org

Charity Number: 3628

Or by e-mail to: dataprotection@.....