# Focolare GB Data Protection: Policy and Procedures

*This Policy should be read in conjunction with:*

*- the* **Focolare GB Privacy Statement** *which is published on Focolare GB website: https://www.focolare.org/gb/privacy-2/*

*- the* **Focolare GB Retention Policy**

| | |
|---|---|
| Prepared by | Gerry Murphy and Claudia Melis - reviewed on 22nd September 2023 with Data Protection Team (Ana Siewniak, Anne Howes, Patricia Batista, Sylwia Machej). Based on the version prepared with contribution from Christina Kennedy. |
| Approved by the Focolare Trust Trustees and Mariapolis Ltd Directors - Date | 28th October 2023 |
| Date of next review | 31st October 2025 or earlier if needed due to legislation or organisational changes. |

# CONTENTS

# Aim of this Document

The aim of this document is to ensure that Focolare GB:

- Complies with data protection law and follows good practice.
- Protects the rights of Focolare GB members, volunteers, associates, participants, staff, customers and partners.
- Is open about how it stores and processes individual data.
- Protects itself from the risk of a data breach.

# Data Protection Law

The Data Protection Act 2018 (DPA) is a domestic law governing the use of personal data and the flow of information in the United Kingdom.

The General Data Protection Regulation has been kept in UK law as the UK GDPR[1].

The Focolare GB will monitor changes in legislation following Information Commissioner's Office (ICO) guidance.

A summary of Data Protection law and principles can be found in Appendix 1.

# People, Risk and Responsibilities

## Scope of this procedure

This procedure applies to Focolare houses and centres including home offices and workplaces.

It applies to all members of all sections, branches and groups which make up the Focolare Movement. It includes any person who takes on a responsibility for a Focolare group (e.g., a 'Word of Life group', a group of interest, a local community group) or a responsibility for a specific event which involves collecting, handling and storing personal data.

*For the purpose of this document, 'Focolare members' refer to all above.*

This procedure also applies to staff and volunteers of the Centre for Unity and New City publishing house.

[1] "On 28 June 2021, the EU approved adequacy decisions for the EU GDPR and the Law Enforcement Directive (LED). This means data can continue to flow as it did before, in the majority of circumstances. Both decisions are expected to last until 27 June 2025. The General Data Protection Regulation has been kept in UK law as the UK GDPR". (see: Overview – Data Protection and the EU | ICO ).
"The GDPR is retained in domestic law as the UK GDPR, but the UK has the independence to keep the framework under review. The 'UK GDPR' sits alongside an amended version of the DPA 2018." (see: The UK GDPR | ICO)

## Data Protection Risks

Focolare GB recognises there are risks associated with dealing with personal data. Mishandling an individual's data could harm that person in some way. In addition a failure in data handling could damage the reputation of Focolare GB as a trustworthy organisation. Risks associated when handling data include:

- **Data Breaches**. For instance, information being lost, or shared or given out inappropriately. (See section 7).
- **Failing to offer choice**. For instance, all individuals should be free to choose how the Focolare uses data relating to them.
- **Failing to respect individuals' rights**. For instance, failing to update an individual's contact details.
- **Failing to communicate transparently** how the Focolare GB collects, handles and stores personal data.
- **Reputational damage**. For instance, Focolare could suffer if hackers successfully gained access to sensitive data.

## Responsibilities and Accountability

Focolare GB members have some responsibility for ensuring that data is collected, stored and handled properly.

However, these people have key areas of responsibility:

- The *Governing Bodies* of The Focolare Trust and Mariapolis Ltd are ultimately responsible and accountable for ensuring that Focolare GB meets its legal obligations.
- The *Data Protection Officers* i.e., Claudia Melis and Sylwia Machej, together with the Data Protection Team (Ana Siewniak, Anne Howes, Gerry Murphy and Patricia Batista) are responsible for:

  Governance and Training
  - Keeping the Governing Bodies 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 procedure.
  - Dealing with requests from individuals to see/update/delete/transfer the data that Focolare GB holds about them (see Section: Subject Access Requests and other rights of the individual).

  Evaluation and Monitoring
  - Ensuring that all IT systems, services and equipment used for storing data meet acceptable security standards.
  - Performing regular checks and scans to ensure security hardware and software is functioning properly.
  - Evaluating any third-party service that Focolare GB is considering using to store or process data.

  Publicity and promotion
  - Approving any data protection statements attached to communications such as emails and letters.
  - Where necessary, with other relevant members of Focolare to ensure that publicity initiatives abide by data protection principles.

The Data Protection team carries these responsibilities liaising with the Communication team and IT advisers of Focolare GB.

To fulfil the above duties the members of the data protection team to Focolare GB are themselves required to undertake regular, on-going, documented training. Those trained will disseminate Data Protection information to other members as necessary to ensure compliance with GDPR by all.

# General Guidelines

## Collecting Personal Data

Focolare GB collects personal data for specific purposes (e.g., Newsletter distribution). The collection of data may be taken in different ways:

- Third Party email provider (Mailchimp) subscription form
- Consent forms e.g., parental consent forms for young people or event registration forms
- Personal contact, via email or phone/text

Focolare GB appreciates that when collecting personal data, it is necessary to explain the purpose for which it is being collected and who will be using it, and make sure that the personal data is limited to what is necessary in relation to the purposes for which it is processed.

Any collection of personal data by members of Focolare should follow the GDPR principles outlined in Appendix 1 and always be conducted in line with the Focolare GB Privacy Statement, which can be found on the Focolare GB website:
https://www.focolare.org/gb/privacy-2-2/

It is recommended not to use social media as a way of *collecting* personal data.

### Photos, videos, audio recordings

Photos, videos or voice recordings are personal data. Photographs and other forms of recording may occur during Focolare GB events. Used appropriately they can enhance the enjoyment of those participating and explain to others the nature of these events. In addition, as a charity, Focolare GB should provide evidence of how its funds are being used. For these reasons the Focolare GB has a legitimate interest in obtaining such images/recordings.

This legitimate interest notwithstanding, participants at Focolare GB events have the absolute right to 'opt out' of having such recording of themselves made. All Focolare GB events will remind participants of this right and have procedures in place to ensure this 'opt out' is recorded and enacted.

Photos/recordings of children and vulnerable adults required particular sensitivity in handling. For this reason, explicit consent should be sought from a parent/carer prior to any such photos/recordings being made.

## Handling Personal Data

Focolare GB has procedures in place to ensure that personal data will be used only for the purpose stated when collected.

An individual's consent would be sought before using data for a different purpose or sharing it with people/organisations other than the ones stated when the data was collected.

When working with personal data, Focolare members will take reasonable measures to keep it secure (See Appendix 2 for more information).

They should take reasonable steps to ensure that data is kept accurate and up to date.

Data will be updated or removed from the system should it be found to be inaccurate.

## Sharing Data with Third Parties

Focolare does not share personal data with any other organisation, public body or commercial organisation, unless Focolare GB has a legitimate interest to do so, for example when using a third party to deliver a product or service such as for emailing (see section 3 of Focolare GB Privacy Statement: https://www.focolare.org/gb/privacy-2/).

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Focolare GB will disclose the requested data. However, the Data Protection team will ensure the request is legitimate, seeking assistance from the Governing Bodies and from a legal advisor where necessary.

Other reasons for disclosing personal data without the individual consent include vital interest (e.g., medical emergency) or public interest (e.g., reporting a safeguarding allegation to the police).

Focolare GB may share data with Parties outside the UK, for example when using Mailchimp (mailing provider) or when organising international events such as 'Genfest' to enable the use of email services and participation in international events. Information will only be shared with organisations outside the UK who have provided a satisfactory statement of privacy (Privacy Policy).

Individuals have the right to request a copy of any agreement under which personal data is transferred outside of the UK.

## Storing Data

Data will be held in as few places as necessary. Appendix 2 of this procedure document describes how and where data should be safely stored. Focolare GB members will comply with this guidance.

Questions about storing or destroying data safely should be directed to the Data Protection Team as appropriate.

The Focolare Data Protection Team is working on a Data Retention Schedule (by 1st December 2023) which will determine how long different documents containing personal data should be stored for.

# Subject Access Requests and other rights of the individual

All individuals who are the subject of personal data held by Focolare GB have certain rights that all must respect:

- **The right of access** – seeing what information Focolare GB holds about them (Subject Access Request, or SAR). "An individual can make a SAR verbally or in writing, including on social media".[2]
- **The right of rectification** – updating their data.
- **The right of erasure** – deleting their data.
- **The right to restrict processing** – limiting the use That Focolare GB makes of their data.
- **The right to object to processing** – objecting to their data being used for a specific purpose, such as direct marketing.
- **The right of portability** – having a copy of their data in a 'portable format' so that other organisations can use it.

In addition to these points, individuals have the right to:

- challenge processing which has been justified on the basis of our legitimate interests or in the public interest.

The Data protection Team will always verify the identity of anyone making a SAR or another of these requests before handing over any information.

Any Focolare Member who was made aware of a SAR or another of these requests, should contact promptly the Data Protection team, by phone (07443 873717) or by email (dataprotection@focolare.org.uk). (The Focolare GB has to comply with a SAR without undue delay and at the latest within one month of receiving the request.)

## Providing Information

All individuals who are the subject of personal data held by Focolare GB are also entitled to be informed of how Focolare GB is meeting its data protection obligations.

Focolare GB aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights as outlined above.

To these ends, Focolare GB has a privacy statement on its website https://www.focolare.org/gb/ setting out how data relating to individuals is used by them. (A printed copy of the statement can be made available on request).

[2] Right of access | ICO More info. on individual rights can be found here: A guide to individual rights | ICO.

# Data Breaches

A breach is when personal data is being lost, stolen, deleted, shared with or accessed by unauthorised people. Some examples of data breach:

- Emailing personal data to the wrong person.
- Leaving printouts containing personal data which could be accessed by third parties.
- Leaving documents in the boot of a car which is then stolen.
- Posting personal information on social media without permission.
- Letting someone else use a personal account or password.
- Losing a memory stick containing personal data.
- Being overheard discussing sensitive personal data.
- Computer being hacked.

If Focolare members discover a data breach they should:

1. **Report it promptly** to the Data Protection team by Email: dataprotection@focolare.org.uk ; or by Telephone: 07443 873717 or 07729 541 996.

   If in doubt, they should report it. The law requires keeping a record of all actual and potential breaches.

2. **Minimise the impact**. For example:
   - If the member has lost a memory stick containing personal data, they should go back and see if they can find it (they will need to report the breach even if it is recovered).
   - If someone found the member's password to their email account, they should change it.
   - If a photo was posted on social media without consent, this should be deleted.
3. **Follow up any other actions** agreed with the Data Protection team, these may consist of:
   - Contacting the people whose personal data has been affected.

4. **Reviewing processes** - how the member handles personal data.

The Data Protection Officer (DPO) will assess whether the Data Breach needs to be reported to ICO (within 72 hours of the incident being notified) and whether the Data Subjects of the personal Data breach need to be informed (without undue delay).

The Data Protection Team will keep a register of Data Breaches incurred and document decisions.

---

**FOCOLARE GB DATA PROTECTION TEAM:**

Claudia Melis (DPO), Sylwia Machej (DPO), Gerry Murphy, Ana Siewniak, Anne Howes, and Patricia Batista.

For help, support or advice on data protection, queries or complaints contact: dataprotection@focolare.org.uk or write to the following address:

67 Church Road, Roby, Liverpool L36 9TN

Further advice and information can be obtained from the Information Commissioner's Office at www.ico.org.uk .

# Appendix 1. Summary of Data Protection Law

Data Protection Law describes how organisations must collect, handle and store personal information.

Personal information is understood to be information by which a living person can be identified directly, or indirectly by collating information. It can include names and addresses, telephone numbers and emails, NHS and Passport numbers, photos, images and voice recordings.

Data protection law also covers sensitive data which can include a person's ethnicity, philosophy or religion, health status, sexual orientation etc.

The law applies to the processing of information that is partly or wholly by automated means; and to information however collected that forms part of or is intended to form part of a filing system.

These rules apply therefore, regardless of whether data is stored electronically, on paper or on other materials or devices.

## Data Protection Principles

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

| Data Protection is underpinned by important principles: | These say that personal data must: |
|---|---|
| ● Lawfulness, fairness and transparency | Be processed fairly and lawfully, in a transparent way |
| ● Purpose limitation | Be obtained only for specific, lawful purposes |
| ● Data minimisation | Be adequate, relevant and not excessive |
| ● Accuracy | Be accurate and kept up to date |
| ● Storage limitation | Not be held for any longer than necessary |
| ● Integrity and confidentiality (security) | Processed with confidentiality, in accords with the rights of the data subjects and protected in appropriate ways |
| ● Accountability | The Data Controller (Focolare GB) is responsible for complying with the UK GDPR and must be able to demonstrate compliance. |

# Appendix 2. Data Protection Guidelines

a. Always seek the person's consent before sharing their personal information.
b. Follow the Focolare GB Policy for keeping and sharing information safely.
c. If you lose any personal information or share it by mistake, report it promptly to the responsible of the local Focolare or the Data Protection Team (dataprotection@focolare.org.uk). If in doubt, report it.
d. Always explain who you are and why you are collecting the information.
e. Collect and record only what you need for your purpose.
f. Only provide information that is necessary and consider minimising the data you need to share. For example, consider sharing first names or initials only, rather than specifying surname, date of birth, location etc.
g. Always check if you have permission before sharing any personal data with somebody else or posting it on media.
h. Make sure the information you hold about people is accurate and updated.
i. Keep personal information in a secure place.
j. Delete photos/video/audio and any back-ups from your device(s) once you have used them for the agreed purpose.

# Appendix 3. Information security guidelines

### Sending post / handling paper documents

a. If you are sending documents containing personal data via post, address the envelope as 'confidential' and always use a 'tracked service', such as recorded or special delivery.
b. Paper documents containing personal data should be stored in a secure place and only be accessible to authorised people.
c. Considerable amount of personal data (e.g., list of local community contacts) and any sensitive data should be stored in a locked cupboard.
d. You should make sure that papers and printouts are not left where unauthorised people could see them, like on a printer.
e. Data printouts should be shredded and disposed of securely when no longer required.

### Using emails

a. Never use a shared email address (e.g., janeandtom@gmail.com) to collect or handle personal data. Some Focolare members for their role with Focolare communicate with many people and handle a considerable amount of data. These members should use a focolare.org.uk email address for their role.
b. Make sure you use the BCC field for group emails.
c. Always start a fresh email. Emails can contain long conversation chains which are a very common risk for data breaches.
d. Information sent electronically should be encrypted or password protected. When the email is used to send personal information, this should be included not in the body of the email, but in a password-protected attachment. The password should be communicated to the recipient using a different mean (e.g., a text message). If this is not possible, the password should be sent in a new email.
e. Regularly review your inbox and delete historic emails containing personal data no longer needed.

### Downloading / storing files on electronic devices

a. Never download personal data on a public computer (e.g., a public library computer), unless this is extremely necessary (in this case, immediately delete the downloaded file once this has been dealt with, make sure you delete it also from the 'recycling bin').
b. Delete your file from the Downloads folder after the personal data has been dealt with or saved in a secured location on your device.
c. If you share your device with someone else, make sure they cannot access personal data (e.g., password-protecting documents).
d. Your devices (laptop, tablet, mobile etc.) should be protected by a password or a pin.
e. All devices and computers containing data should be protected by approved security software and a firewall.
f. Removable media like USB memory sticks and hard drives containing personal data should be encrypted (for example using BitLocker – encryption programme available on Windows10). If this is not possible, they should be kept locked away securely when not being used.
g. Regularly review and delete the data that is held on your devices.

## Using cloud storage

Documents containing a considerable amount of personal data, e.g. list of local communities contacts, Mariapolis/youth events attendance lists should be stored on the Focolare GB OneDrive Cloud storage.

Other cloud storage such as Google Drive or OneDrive may be used to store information for a temporary period of time, provided that access is restricted only to the relevant people and measures are in place to keep files secure. Considering the following:

a. Choose strong passwords for your (Google/Microsoft) Account and change them frequently.
b. If you share a computer, sign out of your (Google/Microsoft) Account when you have finished.
c. Make sure you understand your automatic back-up system – if this is in place – and particularly where your files are being stored (is your back-up system saving files on your local computer?).
d. If you want to share your files with others, use a link rather than making files public.
e. Make sure you understand the access given to people you are sharing the documents with (have they got access to only one file or the whole folder? Have they got permission to edit the document or only to view? Are viewers able to download the file?)
f. If files contain personal information, ask those it is being shared with not to share the link with anyone else.