GDPR Policy

Table of Contents

Introduction 1

Legal Framework 2

Related Policies and documents 2

Data Protection Principles 2

Individual Rights 3

Definitions 3

Roles and responsibilities 3

Data Processing at Own My Life 4

Use of Imagery / Video 4

Best Practice Principles 5

Confidentiality 6

Data Breach 6

Data Retention 6

Useful Contacts 7

Version Control 7

Introduction

The Women's Liberation Collective is a Charity registered with the Charity Commission; we provide governance for Own My Life.

We recognise that mishandling of data (breaches of GDPR) have the potential to cause distress for the individuals concerned, alongside the risk of reputational damage to Own My Life.

It is therefore important that anyone working on behalf of Own My Life understands the part they play in managing data effectively.

Purpose

The purpose of this policy is to ensure that The Women's Liberation Collective processes personal data lawfully, transparently, and securely in compliance with data protection legislation.

Scope

This policy applies to:

- All employees, contractors, and third parties.
- All personal data processed by Own My Life.
- All systems and applications used by Own My Life.

Legal Framework

This policy is written in accordance with the following legislation.

- Data Protection Act (2018).
- General Data Protection Regulation (GDPR).

The GDPR came into force in 2018, replacing the Data Protection Act. It introduced stricter rules around how organisations collect or process the data of individuals. There are particular requirements relating to data that is considered sensitive, for example health or medical information, or data that is collected in regards someone's political opinions or religious beliefs.

The Information Commissioners Office (ICO) has the ability to impose significant fines upon organisations that fail to comply with GDPR.

Related Policies and documents

- Confidentiality Policy.
- GDPR Policy Statement / Privacy Notice (on Own My Life website).
- Tech Policy.
- Social Media Policy.

Data Protection Principles

Anyone responsible for using personal data must make sure the information is:

- Used fairly, lawfully and transparently.
- Used for specified, explicit purposes.
- Used in a way that is adequate, relevant and limited to only what is necessary.
- Accurate and, where necessary, kept up to date.
- Kept for no longer than is necessary.
- Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

Individual Rights

We recognise individuals' rights to:

- Be informed about how their data is being used.
- Access their personal data.
- Have incorrect data updated.
- Have data erased.
- Stop or restrict the processing of their data.
- Data portability – individuals can ask for a copy of the information we hold about them and use it with another service if they choose.
- Object to how their data is processed in certain circumstances.

Definitions

DEFINITION & EXAMPLE	
Data Controller	An individual / organisation that determines how and why personal data is processed, in this case, The Women's Liberation Collective.
Data Processor	An individual or organisation that processes personal data on behalf of a data controller. For example, staff or volunteers working as part of Own My Life.
Data Subject	An individual whose personal data is being processed. For example, and individuals who undertake facilitator training.
Data Protection Officer (DPO)	The nominated individual responsible for ensuring the organisation is compliant with data protection legislation.
Processing	Any action carried out with personal data, including collection, storage, use, and disclosure.
Personal Data	Any information that can identify a living individual, such as their name, address, or email address.
Sensitive Personal Data	Personal data that requires extra protection, for example health information or ethnic origin.
Direct Marketing	Any communication aimed at promoting a product or service directly to an individual.
Valid Consent	Consent given freely, specifically, and informed. It can be withdrawn at any time – for example consent given for group photo taken at end of each facilitator training session.

Roles and responsibilities

The Women's Liberation Collective Board of Trustees are responsible for:

- Overall compliance with GDPR requirements.

- Ensuring this policy is kept up to date and reflects how the organisation handles data.
- Monitoring the effectiveness of this policy.

The CEO is responsible for:

- Ensuring that staff, volunteers, and contractors are aware of this policy and receive appropriate data protection training.
- Promoting a culture where data protection and confidentiality are taken seriously.
- Reporting any breaches of this policy to the Board of Trustees and where necessary, the ICO.

All staff, freelance contractors and volunteers working on behalf of Own My Life are responsible for:

- Complying with this policy.
- Handling responsibly any data processed on behalf of Own My Life.
- Reporting any breaches of this policy to the CEO / DPO.

Data Processing at Own My Life

The way we process the data of specific individuals or groups is:

- Organisation details: These are used for orders, our public map, invoices, sometimes for posting out training materials. We also record adherence to Expectations of Sisterhood.
- Facilitator training: who has attended training and if applicants are entitled to e-Hub access. Any individual adjustment or support needs are collected, but not retained.
- Personnel records: Placed on our personnel register and records kept for those who have access to our charity Google Drive and other files.
- Donors: We keep a list of their details in order to thank them for their donation.
- Trustees: Placed on our Trustee register.
- Contacts: We sometimes introduce women (who contact us seeking help) to Own My Life organisations who may be able to provide courses for them.
- Details relating to an individual or organisation that are provided in the context of safeguarding or a complaint.

Use of Imagery / Video

Whilst we may take photographs or video recordings to promote our work, we will not take or use photographs in a way that is intrusive or inappropriate.

We will inform individuals in advance if photography or filming is likely to take place, giving them ample opportunity to decline being filmed / photographed. We will advise participants that whilst Own My life will not share images with third parties, we are unable to prevent others from doing so.

We process images in accordance with this policy by ensuring the following:

- We will obtain consent where images clearly identify a person. Consent can be withdrawn at any time.
- We will only use images for the purposes for which they were collected.
- We will not use full names alongside images unless we have explicit permission to do so.
- We will store digital images securely.
- We will only retain images for as long as they are needed. We will then delete them in line with our data retention procedures.
- We will not share images with third parties.

Best Practice Principles

Own My life has developed the following best practice principles to ensure that we manage data securely.

All staff, volunteers, freelance contractors, and Trustees working on behalf of Own My Life must follow these principles. Failure to do so may lead to disciplinary action / us ending our contract with you.

Storing Data securely

- Lock away paper records / notebooks when not in use.
- Use two factor authentication (2FA) on devices.
- Use strong passwords and change them regularly.
- Do not share passwords / login details with partners or family members.
- Do not access data on shared devices (family laptops).
- Ensure screens are locked when not at your computer.
- Save documents in the Own My Life Google Drive.
- Do not save files on personal devices or USB sticks.

Sharing Data safely

- Take time to check email recipients before sending, especially if replying to a thread / conversation.
- Do not send any personal data unless authorised to do so.
- Delete emails / messages containing personal data once no longer needed.

- Do not share any confidential information on social media.

Specific precautions when remote working

- Do not use public Wi-Fi networks.
- Keep papers and devices secure – especially when travelling.
- Do not work on confidential information when in public spaces (cafes / trains) or anywhere that work may be seen.
- Be mindful of conversations that may be overheard – this includes by family members or housemates.

Confidentiality

Personal information
All personal information handled by Own My Life should be treated as strictly confidential.

Staff, trustees, and volunteers must only access or use personal data where it is necessary for their role and must not disclose information to any unauthorised person.

Business sensitive information
You are required to uphold confidentiality about any information that could be considered sensitive, such as financial information or the future plans of Own My Life.

Data Breach

A data breach refers to any incident that has (or could) lead to the accidental sharing or loss of personal data.

Any breach, or suspected breach, must be reported to the DPO within 24 hours, who will then investigate.

The DPO will advise who else may need to be informed. This could include:

- The data subject.
- The Board of Trustees.
- The ICO (within 72 hours of the breach).

Whilst a potential outcome from investigation might be improvements to processes, it could also result in disciplinary action in cases whereby due policy has not been followed.

Data Retention

Data will only be retained for as long as there is an administrative need to do so in order to enable Own My Life to carry out our functions, or for as long as we are required to demonstrate compliance for audit purposes or to meet legislative requirements.

TYPE OF RECORD	RETENTION
Financial records	6 years after the end of the accounting year to which they relate
Facilitator Training Records	Until they ask us to remove them.
Personnel Records (including volunteers / freelance contractors)	6 years after leaving employment
Recruitment Records	Unsuccessful candidates – 3 months Successful candidates – as per personnel records

Useful Contacts

Data Protection Officer (DPO)	CEO / Natalie Collins	07898 138162 natalie@ownmylifecourse.org
Information Commissioners Office (ICO)		www.ico.org.uk

Version Control