# Data Protection Policy

This document is a statement of the aims and principles of Women's Community Matters for ensuring the confidentiality of sensitive information relating to staff, trustees, volunteers and other users of the Centre.

## Introduction

Women's Community Matters needs to keep certain information about its employees, trustees, volunteers and other users to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information so that staff and volunteers can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

To do this, Women's Community Matters must comply with the data protection principles which are set out in the Data Protection Act 1998.

In summary these state that personal data shall:

1. Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
2. Be obtained for a specified and lawful purpose and shall not be processed in any manner not in line with that purpose.
3. Be adequate, relevant and not excessive for that purpose.
4. Be accurate and kept up to date.
5. Not be kept for longer than is necessary for that purpose.
6. Be processed in accordance with the data subject's rights.
7. Be securely protected from unauthorised access, accidental loss or destruction.
8. Not be transferred to a country outside the European Economic Area, unless that county has equivalent levels of protection for personal data.

Women's Community Matters and all staff or others who process or use personal information must ensure that they always follow these principles. In order to ensure that this happens, Women's Community Matters has developed this Data Protection Policy.

## Status of this Policy

This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the organisation from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

Any member of staff, volunteer or other individual who considers that the Policy has not been followed in respect of personal data about himself or herself should raise the matter with the Designated Data Controller initially. If the matter is not resolved it should be raised as a formal grievance.

## The Data Controller and the Designated Data Controllers

Women's Community Matters as a corporate body is the Data Controller under the 1998 Act, and the Trustees are therefore ultimately responsible for the implementation of the Data Protection Policy. However, the Designated Data Controller will deal with day to day matters.

Women's Community Matters has appointed The Senior Officer to act as the Designated Data Controller. Any queries will regards to this policy and compliance with the 1998 Act should be referred to the Senior Officer.

## Responsibilities of Staff

### Staff information

All staff are responsible for:

• Checking that any information that they provide to Women's Community Matters in connection with their employment is accurate and up to date.

• Informing Women's Community Matters of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. Women's Community Matters cannot be held responsible for any errors unless the staff member has informed Women's Community Matters of such changes.

### Data Security

When, as part of their responsibilities, staff and volunteers collect information about other people they must comply with the Data protection Act 1998 and this policy.

All staff are responsible for ensuring that:

• Any personal data that they hold is kept securely, for example, computerised data should be password protected; and

• Personal information is not disclosed either orally, in writing, via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

## Rights to Access Information

All staff, volunteers and users of the service have a right under the 1998 Act to request access to any personal data being kept about them either on computer or in certain files. Any person who wishes to exercise this right should complete a Subject Access Request in writing and submit it to the Designated Data Controller.

Where data is requested, Women's Community Matters may charge £10 on each occasion that access is requested.

Women's Community Matters aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 calendar days, as required by the 1998 Act.

## Subject Consent and Processing Sensitive Information

### Personal Data

Women's Community Matters has to process personal information to efficiently manage its day to day operations and operate other policies.

Agreement to Women's Community Matters processing some specified types of personal data is a condition of acceptance of employment for staff. This includes information about previous criminal convictions.

In many cases, Women's Community Matters can only process personal data with the consent of the individual.

In some cases, if the data is sensitive, as defined in the 1998 Act, express consent must be obtained. Processing Sensitive Information - sometimes it is necessary to process information about a person's health, criminal convictions, or race. This may be to ensure that Women's Community Matters is a safe place for everyone. Because this information is considered sensitive under the 1998 Act, staff will be asked to give their express consent for Women's Community Matters to process this data. An offer of employment may be withdrawn if an individual refuses to consent to this without good reason.

Certain items of information relating to Women's Community Matters staff will be made available via searchable directories on the public Web site, in order to meet the legitimate needs of researchers, visitors and enquirers seeking to make contact with Women's Community Matters.

Personal information should:

- Be kept in a locked filing cabinet, drawer, or safe; or
- If it is computerised, be coded, encrypted or password protected both on a local hard drive and on the network drive that is regularly backed up; and
- NOT be kept on removable storage media.

**Examples of data**

**Personal data**

Definitions of personal data are highly complex, and it is difficult to define categorically. However, broadly speaking and in day-to-day use, 'personal data' is information which relates to a living, identifiable individual.

In the context of this document and the Women's Community Matters requirement to process 'personal data' as part of its duty of care and to support women and volunteers, 'personal data' may include:

- access and attendance registers information

• ongoing contact information records
• reports to funders on the progress of participants
• reports and information shared with partner organisations
• staff records, including payroll records
• disciplinary records
• personal information for delivery of course/activity purposes
• records of contractors and suppliers

It is necessary for Women's Community Matters to process certain personal data to fulfil its obligations.

**Exemptions**

Certain data is exempted from the provisions of the Data Protection Act, example include:

• The prevention or detection of crime
• The assessment of any tax or duty
• Where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the Women's Community Matters
There are other exemptions under the act.

**Retention of Data**

Women's Community Matters has a duty to retain some staff, volunteer and client personal data for a period of time following their departure from Women's Community Matters, mainly for legal reasons. Different categories of data will be retained for different periods of time. The time span can be requested in writing from Women's Community Matters.

**Conclusion**

Compliance with the 1998 Act is the responsibility of all members of the Women's Community Matters. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or even to a criminal prosecution.

To be reviewed every 2 years as a minimum.

Version 1 - 23rd March 2021

Version 2 - 1st September 2022

Version 3 – 13 March 2024 SR

Next due for review: March 2026