



**THE MILL ROAD WINTER FAIR ASSOCIATION  
(MRWF)**

**DATA PROTECTION POLICY**

**DATED JANUARY 2011**

**CONTENTS**

**CLAUSE**

Policy statement.....	1
Status of the policy.....	1
Definition of data protection terms.....	1
Data protection principles.....	2
Fair and lawful processing.....	3
Processing for limited purposes.....	3
Adequate, relevant and non-excessive processing.....	4
Accurate data.....	4
Timely processing.....	4
Processing in line with data subject's rights.....	5
Data security.....	5
Dealing with subject access requests.....	6
Providing information over the telephone.....	6
Monitoring and review of the policy.....	6



## **POLICY STATEMENT**

- 1.1 During the course of its activities MRWF will collect, store and process personal information about current, past and prospective members, volunteers, event participants, suppliers, marketing and PR contacts and others with whom MRWF communicates.
- 1.2 This information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 (the Act) and other regulations. The Act imposes restrictions on how MRWF may use that information.
- 1.3 MRWF is a not-for-profit organisation. The MRWF Committee understands that under the Data Protection (Notification and Notification Fees) Regulations 2000 MRWF is exempt from the requirement to register with the Information Commissioner under the Act. However, the MRWF Committee recognises that everyone has rights with regard to how their personal information is handled and MRWF must treat it in an appropriate and lawful manner.

## **STATUS OF THE POLICY**

- 1.4 This policy sets out MRWF's rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.
- 1.5 Anyone who considers that the policy has not been followed in respect of personal data about him/herself or others, or has any other questions or concerns about this policy, should raise the matter in the first instance with either the MRWF Secretary or the MRWF Chair.
- 1.6 This policy will be published on the MRWF website. Hard copies may be requested from the MRWF Secretary.

## **DEFINITION OF DATA PROTECTION TERMS**

- 1.7 **Data** is information that is stored electronically, on a computer, or in certain paper-based filing systems.
- 1.8 **Data subjects** for the purpose of this policy include all living individuals about whom MRWF holds personal data. A data subject need not be a UK

national or resident. All data subjects have legal rights in relation to their personal data.

- 1.9 **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in MRWF's possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as an evaluation).
- 1.10 **Data controllers** are the people or organisations that determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. The MRWF Committee is the data controller of all personal data used in the MRWF organisation.
- 1.11 **Data users** include MRWF Committee members and volunteers whose work involves using personal data. Data users have a duty to protect the information they handle by following MRWF's data protection and security policies at all times.
- 1.12 **Data processors** include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include MRWF Committee members and suppliers or volunteers who handle personal data on behalf of MRWF.
- 1.13 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.
- 1.14 **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 or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned. MRWF does not expect to process any sensitive personal data.

#### **DATA PROTECTION PRINCIPLES**

Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

- (a) Processed fairly and lawfully;
- (b) Processed for limited purposes and in an appropriate way;
- (c) Adequate, relevant and not excessive for the purpose;
- (d) Accurate;
- (e) Not kept longer than necessary for the purpose;
- (f) Processed in line with data subjects' rights;
- (g) Secure; and
- (h) Not transferred to people or organisations situated in countries without adequate protection.

#### **FAIR AND LAWFUL PROCESSING**

- 1.15 The Act is intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is (in this case the MRWF Committee), the purpose for which the data is to be processed by MRWF, and the identities of anyone to whom the data may be disclosed or transferred.
- 1.16 For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In most cases the data subject's explicit consent to the processing of such data will be required. MRWF does not expect to process sensitive personal data.

#### **PROCESSING FOR LIMITED PURPOSES**

- 1.17 Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.
- 1.18 MRWF will process personal data for the purposes of:
- (a) Establishing and maintaining membership and support for MRWF, including approaching potential event participants and suppliers;

- (b) Providing and administering activities for MRWF's members and regular contacts;
- (c) Volunteer administration;
- (d) Advertising, marketing and public relations in relation to MRWF's activities;
- (e) Keeping accounts and making financial and management forecasts relating to MRWF's activities;
- (f) Deciding whether to accept anyone as an event participant or supplier; and
- (g) Keeping records of purchases, sales or other transactions to ensure that the relevant payments, deliveries, services or events take place.

#### **ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING**

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data that is not necessary for that purpose should not be collected in the first place.

#### **ACCURATE DATA**

- 1.19 Personal data must be accurate and kept up to date. Information that is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.
- 1.20 The members of the MRWF Committee are all responsible for ensuring that the personal data held by MRWF is accurate and up to date. The MRWF Committee will cleanse the personal data held by MRWF at least once every two years.
- 1.21 Anyone who believes that MRWF is holding personal data about him/herself or another person that is inaccurate or out-of-date should contact the MRWF Secretary or the MRWF Chair in the first instance.

#### **TIMELY PROCESSING**

Personal data should not be kept longer than is necessary for the purpose. This means that personal data should be destroyed or erased from MRWF's systems when it is no longer required. If MRWF wishes to retain data for statistical purposes, that data should be anonymised so it is no longer personal data.

## **PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS**

Data must be processed in line with data subjects' rights. Data subjects have a right to:

- (a) Request access to any data held about them by a data controller;
- (b) Prevent the processing of their data for direct-marketing purposes;
- (c) Ask to have inaccurate data amended and
- (d) Prevent processing that is likely to cause damage or distress to them or anyone else.

## **DATA SECURITY**

1.22 MRWF must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

1.23 The Act requires MRWF to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if that data processor agrees to comply with those procedures and policies, or if that data processor puts in place adequate measures.

1.24 Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

- (a) **Confidentiality** means that only people who are authorised to use the data can access it.
- (b) **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
- (c) **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system known as CAMS.

1.25 Security procedures include:

- (a) **Secure access to CAMS:** Access to CAMS is restricted to those individuals with an authorised user name and secure password. Users of CAMS must not disclose their password to anyone else. If users download information from CAMS onto their personal

computer or any form of mobile device, they must ensure that it is password protected and that it is properly disposed of when they have finished working with it.

- (b) **Secure lockable desks and cupboards:** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
- (c) **Methods of data disposal:** Paper documents should be shredded. Floppy disks, CD-ROMs and DVDs should be physically destroyed when they are no longer required. Data on USB sticks, mobile devices, hard drives etc should be properly deleted.
- (d) **Equipment:** Data users should ensure that individual monitors or screens do not show confidential information to passers-by and that they log off from their computer or mobile device when it is left unattended.

#### **DEALING WITH SUBJECT ACCESS REQUESTS**

A formal request from a data subject for information that MRWF holds about them must be made in writing. A fee is payable by the data subject for provision of this information. Any MRWF Committee member or volunteer who receives a written request should forward it to the MRWF Secretary or the MRWF Chair immediately.

#### **PROVIDING INFORMATION OVER THE TELEPHONE**

Any MRWF Committee member or volunteer dealing with telephone enquiries should be careful about disclosing any personal information held by MRWF. In particular they should:

- (e) Check the caller's identity to make sure that information is only given to a person who is entitled to it.
- (f) Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.
- (g) Refer to the MRWF Secretary or the MRWF Chair for assistance in difficult situations. Nobody should be bullied into disclosing personal information.

#### **MONITORING AND REVIEW OF THE POLICY**

- 1.26 This policy and its effectiveness will be reviewed annually, at the first MRWF Committee meeting after the MRWF Annual General Meeting, to ensure it is achieving its stated objectives.