

# **Data Protection Policies and Procedures**

Music in West Kilbride (MiWK) (Registered charity SCO 37517)

## **Data Protection Policies and Procedures**

### Summary

We will only hold information about you as an individual if you specifically consent to us doing so. We will use your personal information only for managing your membership (if you are a member), sending out emails with information about MiWK events and other arts events in West Kilbride, such as the Vertex Festival, and managing ticket sales for concerts. We will NOT pass your information to any other organisation unless required to by law.

### Full Policy

The committee of MiWK recognises its responsibilities under the General Data Protection Regulations (GDPR) and has produced this document to enable compliance with the Regulations and the protection of the personal information of its members and others. This document will be reviewed annually.

### Policies

MiWK is currently exempt from registration with the Information Commissioner but is responsible for complying with GDPR. This exemption will be reviewed annually.

MiWK will only hold personal information that is needed for managing its membership, circulating relevant emails to members and to others who have asked to receive them, and managing ticket sales for concerts.

Personal information will only be held if the individual concerned

(known as a “data subject”) specifically consents to MiWK holding the information. Data subjects will be advised that he/she can withdraw this consent at any time (and how to do this), at which time his/her personal information will be permanently deleted.

Personal information will be carefully protected. The full records of personal information will be held on a single computer, in a password protected computer file. This computer file will not be emailed or otherwise transferred in a non-secure fashion. If any extracted information is needed for a specific purpose it will be prepared as necessary and destroyed as soon as possible after being used. Personal information will not be shared with any person or organisation outwith MiWK, except as may be required by a UK law enforcement agency. Personal information held by MiWK will only be used in pursuit of the objects of MiWK as stated in its constitution.

GDPR requires MiWK to have two named roles:

- The “data controller”. The MiWK committee, acting as a corporate group, will assume this role, which involves determining the purposes and means of processing personal data;
- The “data processor”. MiWK appoints committee member Chris Maughan to this role, which involves keeping and using the personal data.

MiWK’s data protection policy and procedures will be available on request to anyone with an interest in MiWK and will be placed on the MiWK website.

Procedures to be used by the Data Processor:

Password protected computer file

The Data Processor shall maintain a password protected computer file for keeping personal information covered by the GDPR.

The computer file shall be kept on a single computer under the control of the Data Processor.

The password shall be a minimum of 8 characters, including at least two letters and two numbers. It shall be changed at least every six months, or at any time if there is reason to believe that it has been compromised. A copy of the current password shall be sealed in an envelope and kept personally by the Chair of MiWK.

Each record of a data subject in the computer file shall be given a unique record number.

Except as required by a UK law enforcement agency, the Data Processor shall not share the computer file or its contents with any person other than in extracted form as necessary for the purposes of MiWK. The computer file shall not be transferred (for example on change of the Data Processor) by email or other non-secure means. Obtaining consent to keep personal information. Consent shall be obtained before personal information is held. MiWK holds personal information only for the purpose of its club and concert management. The personal information that may be held is:

- For club membership management: forename, surname, address, email address, phone number, start date of membership, amount of membership fee paid
- For news circulation: forename, surname, address, email address
- For managing concert tickets: forename, surname, concert concerned, number of tickets reserved, payment received or outstanding.

Standard text (as defined later in this document) shall be used to obtain consent from data subjects to hold their information and to inform them of their right to withdraw consent at any time. The Data Processor can obtain this consent either electronically or on paper as appropriate, keeping the response from the data subject as a record of his/her consent.

The Data Processor shall retain the record of consent until either (a), it has been replaced by a more recent record of consent, or (b) consent is withdrawn; in either of these events the record shall be destroyed.

### Management of consent

When seeking to obtain consent, the Data Processor shall:

- Ensure that the individual concerned is provided with the standard text

- (where personal information is already held) keep the information in the password protected computer file

- After one month review whether consent has, in fact, been given, at which time any

personal information shall be deleted if consent has not been given.

Personal information could potentially be received by MiWK in a number of different ways (e.g. letter, email, through the website, by phone) and to any one of the committee. On recognising that any personal information is being presented to MiWK, the

committee member concerned shall:

- Pass the information directly to the Data Processor, and
- Inform the individual concerned that this has been done.

The Data Processor shall then ask for consent as outlined above.

### Withdrawing of consent

If a data subject withdraws consent to MiWK holding personal information (or if he/she does not give consent when information is already held) the Data Processor shall:

- Delete from the computer file all information that could personally identify the data subject, leaving in the computer file only the following information:

- o A unique record number

- o The date consent was originally given, or renewed, if any

- Destroy the record of consent (where this is held)

- Update the computer file to show the date that a withdrawal of consent request has been received (or has been assumed because of lack of response from the data subject) and the date it has been actioned

- Inform the data subject that his/her personal information has been

deleted.

This will leave the computer file holding minimum information about that data subject solely for audit purposes – this information cannot identify the data subject.

### Sending emails

Where it is necessary to send an email to a number of data subjects (for example to all members):

- The email content shall be passed by the originator to the Data Processor, who will undertake the actual sending of the email
- The names and email addresses of recipients shall be concealed from other recipients by putting recipients' email addresses only in the BCC field.

### Using extracted information

There will be occasions where information needs to be extracted from the computer file and used by other committee members of MiWK. (A regular example will be for concerts where the committee member keeping the door will need a list of all members, who automatically have right of entry, together with non-members who have reserved a ticket for that concert).

Where extracted information is needed, the Data Processor shall produce the information in an appropriate format (which may be either electronic or physical). Personal information included shall be kept to the minimum needed for the purpose.

In the example above, the door keeper only needs:

- For members, names of currently paid up members, and
- For non-members, their name, the number of tickets reserved, and whether he/she has already paid for their reserved tickets or not.

In particular, personal information not needed for the specific occasion shall not be included. So, in the example above, it would be wrong to include phone numbers, email addresses, etc.

When the specific occasion has been completed, the extracted information shall be destroyed, either by shredding a physical document or by deleting an electronic file. Standard Text to include

when seeking consent (this text can be adapted to suit if necessary, for example where the recipient does not have electronic access)