Data Protection Policy

Version	1.0
Date approved by MMCS Committee	2 August 2024
Review Date	August 2026

1. OVERVIEW

Maidenhead Musical Comedy Society ("MMCS") takes its responsibilities regarding the management of the requirements of the Data Protection Act 2018 (UK GDPR) very seriously. This policy sets out how we manage our responsibilities, in accordance with the Act, to protect the information we collect as part of our business, and should be read alongside our **Privacy Policy for Members & Supports / Privacy Policy for Children**.

2. INTRODUCTION

MMCS obtains, uses, stores and otherwise processes personal data relating to potential, current and former participants, external contacts and contractors, collectively referred to in this policy as "data subjects".

When processing personal data, we are obliged to fulfil individuals' reasonable expectations of privacy by complying with GDPR and other relevant data protection legislation (data protection law).

This policy therefore seeks to ensure that we:

- Are clear about how personal data must be processed and the expectations for all those who process personal data on our behalf;
- Comply with the data protection law and with good practice;
- Protect our reputation by ensuring the personal data entrusted to us is processed in accordance with data subjects' rights;
- Protect us from risks of personal data breaches and other breaches of data protection law.

MMCS's Secretary can be contacted at any time if individuals wish for their personal data to be removed or have any questions about our policy.

3. PERSONAL DATA PROTECTION PRINCIPLES

When processing personal data, MMCS is responsible for, and must demonstrate compliance with, the following data protection principles. Personal data will be:

- Processed lawfully, fairly and in a transparent manner
- Collected only for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed Accurate and kept up to date
- Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data is processed

- Processed in a manner that ensures its security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction, or damage

4. DATA SUBJECTS' RIGHTS

Data subjects have rights in relation to the way we handle their personal data, including:

- Where the legal basis of our processing is consent, to withdraw that consent at any time
- To ask for access to the personal data that we hold
- To prevent our use of the personal data for direct marketing purposes
- To object to our processing of personal data in limited circumstances
- To ask us to erase personal data without delay:
  - If it is no longer necessary in relation to the purposes for which it was collected or otherwise processed
  - If the only legal basis of processing is consent and that consent has been withdrawn and there is no other legal basis on which we can process that personal data
  - If the data subject objects to our processing where the legal basis is the pursuit of a legitimate interest or the public interest and we can show no overriding legitimate grounds or interest
  - If the data subject has objected to our processing for direct marketing purposes
  - If the processing is unlawful
- To ask us to rectify inaccurate data or to complete incomplete data
- To be notified of a personal data breach which is likely to result in high risk to their rights and freedoms
- To make a complaint to the Information Commissioner's Office (ICO)

MMCS must verify the identity of an individual requesting data under any of the rights listed. Requests (including for data subject access) must be complied with, usually within one month of receipt. Any Data Subject Access Requests received must be forwarded to the Secretary promptly.

5. RESPONSIBILITIES

<u>MMCS's legal responsibilities</u>
As the Data Controller, MMCS is responsible for establishing policies and procedures in order to comply with data protection law.

We must ensure that:

- All personal data is kept securely
- No personal data is disclosed, either verbally or in writing, accidentally or otherwise, to any unauthorised third party
- Personal data is kept in accordance with our retention schedule

- Any queries regarding data protection, including subject access requests and complaints, are promptly directed to the Secretary
- Any data protection breaches are swiftly brought to the attention of the Chairman

The Committee is responsible for:

- Understanding their obligations under GDPR Monitoring compliance with GDPR and other relevant data protection law
- Cooperating with and acting as the contact point for the Information Commissioner's Office
- Having due regard to the risk associated with processing operations in the performance of their tasks, taking into account the nature, scope, context and purposes of processing

Creative team responsibilities

MMCS members who process personal data about participants (e.g. directors, choreographers, musical directors) must comply with the requirements of this policy and any legal obligations.

Third-party data processors

Where external companies process personal data on behalf of MMCS the responsibility for the security and appropriate use of that data remains with MMCS.

Where a third-party data processor is used:

- A data processor must be chosen which provides sufficient guarantees about its security measures to protect the processing of personal data
- Reasonable steps must be taken that such security measures are in place
- A written contract establishing what personal data will be processed and for what purpose must be set out
- A data processing agreement must be signed by both parties.

Contractors/Volunteers

MMCS is responsible for the use made of personal data by anyone working on our behalf. Team members who employ contractors, short term or voluntary staff must ensure that they are appropriately vetted for the data they will be processing.

Participants' responsibilities

Participants are responsible for:

- Familiarising themselves with the Privacy Notice provided when they register
- Ensuring that their personal data provided is accurate and up to date.

6. DATA SUBJECT ACCESS REQUESTS (SARS)

Data subjects have the right to receive a copy of their personal data which is held by MMCS. In addition, an individual is entitled to receive further information about the processing of their personal data as follows:

- The purposes
- The categories of personal data being processed
- Recipients/categories of recipient
- Retention periods
- Information about their rights
- The right to complain to the ICO
- Details of the relevant safeguards where personal data is transferred outside the EEA
- Any third-party source of the personal data.

The entitlement is not to documents per se (which may however be accessible by means of the Freedom of Information Act, subject to any exemptions and the public interest), but to such personal data as is contained in the document. The right relates to personal data held electronically and to limited manual records.

7. REPORTING A PERSONAL DATA BREACH

The UK GDPR requires that we report to the Information Commissioner's Office (ICO) any personal data breach where there is a risk to the rights and freedoms of the data subject. Where the Personal data breach results in a high risk to the data subject, he/she also has to be notified. We have put in place procedures to deal with any suspected personal data breach and will notify data subjects or the ICO where we are legally required to do so.

8. RECORD KEEPING

The UK GDPR requires us to keep full and accurate records of all our data processing activities. We must keep and maintain accurate corporate records reflecting our processing, including records of data subjects' consents and procedures for obtaining consents, where consent is the legal basis of processing. Records of personal data breaches must also be kept, setting out the facts surrounding the breach, its effects and the remedial action taken.

9. DIRECT MARKETING

We are subject to certain rules and privacy laws when marketing to our participants and any other potential users of our services. For example, a data subject's prior consent is required for electronic direct marketing (e.g. by email, text or automated calls).

The limited exception for existing customers (e.g. current participants) known as "soft opt in" allows organisations such as ours to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar services and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

We will comply with this right to object to direct marketing by explicitly offering to data subjects in an intelligible manner clearly distinguishable from other information. A data subject's objection to direct marketing will be promptly honoured. If a data subject opts out at any time, their details will be suppressed as soon as possible (this involves retaining just enough information to ensure that marketing preferences are respected in the future).

10. SHARING PERSONAL DATA

In the absence of consent, a legal obligation or other legal basis of processing, personal data will not generally be disclosed to third parties unrelated to MMCS.

Some bodies have a statutory power to obtain information (e.g. regulatory bodies and government agencies) but we will seek confirmation of any such power before disclosing personal data in response to a request (it should also be noted that without a warrant, the police have no automatic right of access to records of personal data, though voluntary disclosure may be permitted for the purposes of preventing/detecting crime or for apprehending offenders. In these cases, we will seek written assurances from the police that the relevant exemption applies). Some additional sharing of personal data for research purposes may also be permissible, subject to certain safeguards.