



# **Marlow Rowing Club:**

## **Messaging Systems Usage Policy**

### **Table of Contents**

<b>1. Purpose .....</b>	<b>2</b>
<b>2. Scope .....</b>	<b>2</b>
<b>3. Policy statements .....</b>	<b>2</b>
<b>4. Email &amp; Messaging usage principles .....</b>	<b>2</b>
<b>5. Email monitoring.....</b>	<b>3</b>
<b>6. Requests For Information, Investigations and Tracking .....</b>	<b>3</b>
<b>7. Custodian.....</b>	<b>3</b>

## **1. Purpose**

- 1.1 The purpose of this document is to define Marlow Rowing Club and Marlow Rowing Club Trading's (the "Club") Messaging and associated Systems usage policy.
- 1.2 It complements the Internet and Social Networking Policy.

## **2. Scope**

- 2.1 The Systems in scope include the Club's email, CiviCRM emailing/SMS, Google workplace suite and associated systems. The Google workspace suite includes:
  - Email
  - Drive
  - Calendar
  - Meet
  - Chat
  - Docs
  - Sheets
  - Slides
  - All other products and services provided.
- 2.2 This policy governs the Club's approach to managing its Systems, ensuring the best interests of both club members, employees and the club are upheld.

## **3. Policy statements**

- 3.1 The Club's Systems shall only be used in accordance with this policy and related guidelines, the Google terms of use and any appropriate legislation.
- 3.2 Club's Systems are controlled by the Club and provided for volunteers, members and employees to use in the furtherance of the Club's aims. At no point do the Club's Systems, or individual accounts within them e.g. email accounts become the sole property of the user.
- 3.3 The Club provides email and other Systems to assist volunteers and employees in the performance of their roles and no personal use of the systems is permitted.

## **4. Email & Messaging usage principles**

- 4.1 In addition to being binding as a Club Rule under the Articles of Association, the use of the Club's email and messaging Systems indicates acceptance of the policy.
- 4.2 It must be remembered that standard email is not a secure form of communication. The messages that you send may be sent over networks owned by other people and can be intercepted and read by someone else. A secure method of communication must be used if the content of an email is sensitive (e.g., it contains sensitive personal information), such that if its content were disclosed to or modified by an unauthorised person, it could cause harm or distress.
- 4.3 All emails will be treated as Club correspondence and as such will be filtered, recorded and archived at the discretion of the Club.
- 4.4 Users must not register any Club email address with any site or system that is not Club related, such as a personal Facebook / Ebay account. Note that under the Internet and Social Networking Policy, contains controls on setting up social networking site that are Club related.
- 4.5 The Club reserves the right to purge identifiable personal email to preserve the integrity of the email systems.
- 4.6 No user will send, forward, or receive emails that in any way may be interpreted as insulting, disruptive or offensive by any person or company. Note that the Club "Conduct, Disciplinary Process, Bullying" policy imposes rules in relation to conduct and these rules apply to conduct via Club Systems.

- 4.7 Where a volunteer post or employed position is provided with a Club email, it, rather than a personal account, must be used for Club matters.
- 4.8 All email traffic, including attachments, can be monitored and reviewed, and any disciplinary action deemed appropriate will be taken.
- 4.9 All users must ensure compliance with all relevant legislation when using the Club's Systems.
- 4.10 All documents and messages created and sent via the Club's email system are owned by the Club and not by individuals.
- 4.11 Users must not forward chain letters either internally or externally. This includes those purporting to be for Charity or other good causes as well as those promising wealth or other personal gain. Virus warnings come under the same exclusion as the majority of these are false. Employees must refer to the IT Officer to check the validity of such messages but must not forward these messages to anyone else inside or outside the Club under any circumstances.
- 4.12 Email addresses must not be disclosed unnecessarily. Emails sent to groups or distribution lists should put those lists in the "bcc" recipients and not disclose email addresses from one member to another. See also the Club Data Protection Policy.
- 4.13 Information provided in surveys or other questionnaires may lead to risks such as receiving unwanted junk messages.
- 4.14 Users must not subscribe to email lists unless they are Club related. The volumes of messages that can be generated are high and the content may be dubious resulting in conflict with the conditions stated above.
- 4.15 Emails and attachments should not be opened unless they are from a known source. Caution must also be exercised even if attachments are received from a known source but are unexpected.

## **5. Email monitoring**

- 5.1 The Club's email facilities will be monitored in accordance with:
- this policy and related guidelines
  - All appropriate legislation – including the Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000 and The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

## **6. Requests For Information, Investigations and Tracking**

- 6.1 The Head of IT and one Director can authorise access to email accounts in the circumstances described below:
- *Absence.* Where an email account holder is an employee absent from work or a volunteer post holder away from the club, authorisation can given for other members to have access to their email. Normally such access should only be sought for absences in excess of ten working days. The "owner" of the email should be informed immediately access is allowed.
  - *Investigations.* Where an investigation is being undertaken which could result in a Gross Misconduct, requests need to be formally approved by two directors
- 6.2 Tracking. Where an email needs to be tracked to identify where it has been sent, requests need to be formally approved by two Directors.

## **7. Custodian**

- 7.1 It is the responsibility of the Club's IT Officer to ensure that this policy is regularly reviewed and updated.

## **Version Control**

This document is version 1 of the Policy, approved on 13<sup>th</sup> March 2023 and supersedes any previous policies. This document is a Rule of MRC created under Article 65 of the Articles of Association and is binding on employees, members and volunteers.