Standard Operating Procedure (SOP)

21
CLUB DIGITAL MEDIA and AI POLICY

Introduction

1. The purpose of this document is to define the Military Brotherhood MMC (MBMMC) social media.

2. Policy for the Club nationally.

3. The MBMMC Media Policy must be used in conjunction with the MBMMC Constitution.

4. Social media refers to interactions among people in which they create, share, and/or exchange information and ideas in virtual communities and networks.

5. Social media offers a tool for the MBMMC to inform members and the general community on what is happening in the Club and other activities.

Definitions

6. Social Media may include (although is not limited to):

    a. social networking sites (e.g. Facebook, Google+, LinkedIn, Bebo).

    b. video and photo sharing sites (e.g. Flickr, YouTube, Instagram, Tik Tok).

    c. blogs, including corporate and personal blogs, as well as blogs hosted by media outlets (eg ‘comments’ or ‘your say’ feature on dailytelegraph.com.au).

    d. micro-blogging (e.g. Twitter, Yammer).

    e. wikis and online collaborations (e.g. Wikipedia).

    f. forums, groups, discussion, and bulletin boards (eg Google groups, union forums).

    g. vodcasting and podcasting (e.g. YouTube, Vemo, iTunes).

    h. virtual worlds (e.g. Second Life).

i. instant messaging (including SMS, MMS, Facebook Messenger, iMessage)

j. geo-spatial tagging (Foursquare, Facebook, Google Places).

k. collaborative e-learning sites and technologies, (eg Moodle, Adobe Connect, Blackboard Eluminate).

l. Online review sites and apps.

m. Email.

Accountabilities

7. The Club President or their nominated representative is accountable for the implementation of this policy.

8. The Club President must periodically review the Policy to ensure that it aligns with relevant Club policies and State and Federal legislation and that related guidelines are relevant and up to date.

9. The Club President will regularly inform of any changes to the policy.

10. Each Sub-branch President is accountable for what a member (Service or Sierra Squad) of their Sub Branch places on social media and which is deemed to be inappropriate.

11. Each Sub Branch President then has an obligation to the Club to ensure removal of such inappropriate material.

Legal and Policy frameworks

12. This policy and all associated procedures are supported by the following policy and legislative framework:

a. Club Constitution

b. Privacy Act (All States and Levels).

c. Criminal Codes (All States and Levels).

13. Administrative Transition, Handover, or Disestablishment

- **Resignation or Departure**: Upon a member's resignation or removal from the Club, they must immediately surrender all administrative credentials and remove themselves as an administrator of any Club-related site.

- **Credential Management:** Similar to the management of official email addresses, the Sub-Branch IT Administrator is responsible for controlling and tracking all platform passwords and resets.

- **Disestablishing a Site:** The closure or deletion of any digital platform representing the Club is a formal administrative act that requires prior authorization. A site must only be ceased after the responsible member has officially notified the Sub-Branch Executive or the NEC of the intent to decommission the platform. This requirement ensures the Club can protect its digital legacy, allowing for the preservation of essential records for the National Database and the orderly removal of protected branding before the platform is taken offline.

14. Enforcement and Penalties

- **Refusal to Hand Over Access:** If a departing member refuses to surrender administrative control of a Club site, it will be viewed as an unauthorised appropriation of Club IP.

- **Disciplinary Action:** Such actions may be recorded as a breach of the Club Code of Conduct and may lead to a referral to the Disciplinary Committee for further action, even if the member has already left the Club, to protect the brand from reputational damage.

- **Reporting:** Sub-Branch Presidents must notify the National Treasurer (IT Manager) immediately if they lose administrative access to any official platform to facilitate recovery efforts through the platform provider.

Policy Principles

15. The objective of this policy is to define the operation of social media within the Club at a National level.

16. The behaviour of members using an official Club social media platform that carries the Club logo or name at a National level is defined by the Club Constitution.

17. The personal use of social media where members identify an affiliation with or comment upon the Club, its members, or activities online is defined and regulated by the provisions of the Club Constitution.

18. The MBMMC is a non-political organisation and comments by members of the Club on past, current or future political issues while representing themselves as a member of the MBMMC are not to be included in any form of social media.

Administrative Continuity and Access Control

19. **Mandatory Multi-Administrator Requirement** - To prevent the loss of access to Club digital assets, all social media sites (including but not limited to Facebook, Instagram, Twitter, and TikTok) that represent a Sub-Branch or the National Body must adhere to the following:

    - Minimum Administrators: Where the platform functionality permits, every site must have a minimum of three (3) active Administrators.

    - Composition: These administrators must be current financial members (Service or Sierra Squad) of the relevant Sub-Branch and are directly responsible to the Sub-Branch President.

    - Redundancy: One of the three administrators should ideally be the Sub-Branch IT Administrator or a designated member of the Sub-Branch Executive to ensure that no single individual has sole "creator" authority over the platform.

20. **Ownership of Digital Assets**

    - Club Intellectual Property (IP): In accordance with Constitution Paragraph 247, all sites using the Club's name, logo, or regalia are the property of the MBMMC National Body.

    - **Naming Conventions**: All sites must follow the established naming conventions as detailed in Paragraphs 34 – 35 below. This is to clearly identify these names as official Club assets.

    - **Non-Personal Ownership:** No member may claim personal ownership of a social media site created to represent the Club. The content and access credentials are considered Club property.

Operational use of social media

21. The social media function can be an integral part of Club operations. Its goals are to:

    a. give the Club members information.

    b. inform the public about Club events.

    c. enhance the effectiveness of Club awareness of its activities.

Member Responsibilities

22. All members are to be familiar with and must comply with this policy, and all relevant provisions as documented in the Club Constitution.

23. Members must not be abusive, show disrespect to another member or the Club, nor be disrespectful to any other motorcycle club or member of the public, while using social media. See Paragraph 27 - 30 for conduct expectations and disciplinary procedures.

24. The provisions of the Club Constitution must always be adhered to when members use any form of social media where the Club is referred to, or Club regalia, logos or titles are used.

Establishment of Sites

25. All social media sites that carry the Club logo and are administered by Club members are affected by this policy. Such sites represent the Club and are bound by the Constitution affecting the Club.

Facebook

26. Facebook pages must adhere to the administrator requirements set out in Para 19. These are to be three (3) members of the Sub-branch being made up of Service Members and Sierra Squad Members and are to be responsible to the Sub-branch President for:

    a. Regularly monitoring the content of the site.

    b. Advising the Subbranch Executive of any perceived inappropriate text or graphics that has been uploaded, including posts by non-members or uninvited contributors as outlined in Paragraph 27 – 30.

    c. Removing any inappropriate text or graphics once the Executive has been advised.

    d. The profile picture and page profile information are to incorporate the MBMMC logo. These are to be in the format established in the Constitution of the MBMMC.

Posting Permissions and Member Conduct

27. External Posting Restrictions:

    a. MBMMC-affiliated social media pages, groups, and forums must not allow unvetted individuals (i.e. non-members or those not invited by a verified member) to post

content, comments, or media.

b. Page administrators must:
   i. Approve all new contributors.

   ii. Monitor posts for compliance with Club values.

   iii. Remove or report any content that targets, defames, or harasses veterans — whether MBMMC members or not.

28. Protection of Veterans' Dignity. MBMMC upholds the dignity of all veterans. Posts that denigrate, shame, or publicly accuse another veteran — regardless of Club affiliation — are strictly prohibited. This includes:

    a. Sharing unverified allegations.

    b. Posting identifying photos or personal details.

    c. Using language that incites ridicule, hostility, or harm.

29. Member Accountability and Penalties. Any MBMMC member who uses social media to target, defame, or harass another member may face disciplinary action, including:

    a. Formal warning.

    b. Suspension of membership privileges.

    c. Referral to the Disciplinary Committee for potential expulsion.

    d. If the post leads to third-party threats, reputational damage, or mental distress, the matter may be escalated to legal authorities and recorded as a breach of Club Code of Conduct.

30. Reporting and Remediation. Members who witness inappropriate posts must report them to their Sub-Branch Secretary or State President. Page administrators must act promptly to:

    a. Remove offending content.

    b. Notify the National Executive.

    c. Support affected members, including referral to Welfare Officers if needed.

Twitter

31. Any Club member can establish a Twitter account and is responsible for its content as per the Club Constitution.

You Tube

32. The Club does not discriminate regarding the use of You Tube. Any video demonstrating Club objectives and activities in a positive way are approved for use on You Tube. Any Club member can upload Club content to You Tube but is responsible to their subbranch.

Other Social Media

33. Club members may establish additional social media platforms where these are determined to be in the Club interest and are able to be adequately supported.

Nomenclature and Identifiers

34. All sites are to be named using a set convention as specified in paragraph 35.

35. Military Brotherhood MMC, followed by Sub-branch name.

    a. One example is: Military Brotherhood MMC Sydney Sub-branch
    b. Second example is: Military Brotherhood MMC Adelaide Sub-branch

Email Address Format for Sub Branch Executives

36. Emails are a common means of communication and document transfer within the Club. While it is not feasible for all Sub Branches to adopt a uniform format, the layout provided in paragraph 39 should be followed wherever possible. This will facilitate the transition of email addresses to new members who assume Executive positions after an AGM election or a member's resignation, ensuring uninterrupted email correspondence without the need to change the address for the Sub Branch Executive position.

37. An email address is a unique identifier for an email account that allows members to send and receive emails. It's made up of three parts:
    a. Local part: The username, which is the name chosen to identify the member for sending and receiving emails.
    b. @ symbol: The separator between the local-part and the domain.
    c. Domain: The internet designation for the email host, which can be a company, organization, or government entity.

38. In some cases, Sub Branches may have their own domain; where possible, this should contain "MBMMC" and the Sub Branch name to help identify the emails. In most cases, a third-party email provider such as Yahoo, BigPond, Outlook, etc. will be used, meaning the domain name will be tied to that provider.

39. The local (front) part of the email address should follow the format below:

- Pres.[sub branch]@[domain] eg Pres.Lakes@outlook.com
- VP.[sub branch]@[domain] eg VP. Lakes@outlook.com
- Sec.[sub branch]@[domain] eg Sec.Lakes@outlook.com
- Treas.[sub branch]@[domain] eg Treas.Lakes@outlook.com
- SSM.[sub branch]@[domain] eg SSM.Lakes@outlook.com
- QM.[sub branch]@[domain] eg QM.Lakes@outlook.com
- SSL.[sub branch]@[domain] eg SSL.Lakes@outlook.com
- DC.[sub branch]@[domain] eg DC.Lakes@outlook.com
- RC.[sub branch]@[domain] eg RC.Lakes@outlook.com

40. The Sub Branch should nominate an IT Administrator to manage these email addresses and assist members in setting up their computers and/or mobile phones for Executive email access. The IT Administrator is also responsible for controlling all email address passwords and resets.

Management of Sites

41. All sites are to be managed by nominated members of the relevant Sub-branch. The relevant Sub Branch Executive shall be responsible for overall content of the site, including enforcement of posting permissions and conduct standards as outlined in Paragraph 27 – 30.

Disestablishing a Site

42. A social media site or digital platform representing the Club shall only be closed or deleted after completing the following actions:

- Notification: The responsible member must email a formal intention to cease the site to their Sub-Branch Executive or the National Executive (NEC).

- Credential Finalization: Coordinate with the Sub-Branch IT Administrator to ensure all final passwords and recovery settings are transferred before the account is deactivated.

- Content Compliance: Verify with the Executive that no official records or SITREPs required for the National Database need to be captured prior to deletion.

- Brand Removal: Ensure that the official MBMMC logo and nomenclature are correctly removed if the platform remains active in a personal capacity.

Artificial Intelligence (AI) Usage

Purpose and Scope

43. The Military Brotherhood MMC recognizes the utility of AI in content creation. To safeguard the Club's brand, member privacy, and intellectual property (IP), all members and Sub-Branches must adhere to these safety parameters.

Privacy and Data Security

44. In alignment with **SOP 13, Article 8** and **Constitution Paragraph 301c**, no member shall use AI tools in a manner that compromises personal data.

44.1 **Prohibited Inputs:** It is strictly prohibited to input sensitive member information into public AI models (e.g., ChatGPT, Midjourney). This includes member names, AKAs, medical declarations, Next of Kin (NOK) details, or residential addresses.

44.2 **Administrative Integrity:** AI tools (e.g., Copilot, Gemini) may be used to assist in the **drafting of administrative templates**, structural layouts, and generic wording for official documents, see Paragraph 48 below. However, AI must not be used to generate the final **official Club membership application records** once it contains sensitive member information or to facilitate electronic signatures. In accordance with **SOP 10, Paragraph 6**, the completed application or record must remain a physical document **with handwritten signatures**.

Brand Integrity and Visual Standards

45. The Club operates under "positive instructions" regarding its identity. Per **SOP 3, Paragraph 7**, any design not specifically authorized is prohibited.

45.1. **Logo and Emblems:** AI must not be used to recreate, alter, or "hallucinate" the official Club logo. Official artwork files must be obtained directly from the **National Executive**.

45.2. **Aspect Ratio:** AI-generated visual media must adhere to the official aspect ratio of **0.957:1** to prevent distortion.

45.3. **Colour and Font Compliance:** Patches and regalia image content must match authorized **KingStar Shade 70 (Red)** or **Tasmanian Shade 656 (Khaki)**. Fonts for patches and regalia are limited to **ITC Tiffany**, **Times New Roman**, or **Arial Rounded**.

46. Intellectual Property (IP) and Copyright

- **Ownership:** IAW **Constitution Paragraph 247**, all Club IP remains the property of the MBMMC National Body.
- **Unauthorised Derivatives:** Members are prohibited from using AI to create derivative works of Club regalia, such as "virtual patches" or AI-stylized versions of the Club Number Plate.

47. Content and Conduct

- **Non-Political Stance:** AI tools shall not be used to generate political commentary or advocacy while representing the Club (see **Paragraph 18 above**).
- **Protection of Dignity:** AI-generated media (including "deepfakes") must never be used to denigrate, shame, or ridicule any veteran or member. Such actions constitute a **Category A offence** under **SOP 28**.

Permissible Administrative Uses

48. AI may be used by the National Executive or designated Sub-Branch Executives or authorised member for:

- **Drafting Generic Communications:** Creating templates for non-sensitive notices, such as event announcements or recruitment posters.
- **Editorial Refinement:** Rectifying spelling, grammar, or punctuation errors in draft documents, provided the substance remains unaltered (**SOP 15, Paragraph 9**).

49. Review and Approval

- **National Oversight:** AI-generated media for official recruitment, public websites, or large-scale promotions must be reviewed by the **National Treasurer (IT Manager)** or the **NEC** prior to publication.
- **Fast-Track Provision:** Designs strictly adhering to branding standards may be submitted via the **State President** for fast-track approval.
- **Final Authority:** AI tools are assistants, not authors. The human Executive member remains personally responsible for the accuracy and doctrinal conformity of any document produced with AI assistance.

Further advice

50. Further advice on this policy, including requests for the review of AI-generated media or clarifications on digital branding, should be formally documented and referred to the National Executive (NEC) via the chain of command. Technical inquiries regarding digital asset management or fast-track AI approvals should be directed to the National Treasurer (IT Manager) through the respective State President to ensure consistency with National branding and privacy standards.