Social Media Policy and Procedures

Policy Approved By: Board of Trustees
Date Approved: Jan 2026
Next Review Date: Jan 2027

Responsible Officer: General Secretary

1. Introduction

UMCUK is a registered Charitable Incorporated Organisation (CIO) (Charity Number: 1115442) dedicated to promoting the welfare, culture, religion, education, and health of the Ugandan Muslim community in the UK. As a volunteer-led charity reliant on donations and community engagement, we use social media platforms (e.g., X, Facebook, Instagram, WhatsApp) to communicate with members, share updates on events and initiatives, raise awareness of our work, and foster community integration.

This policy ensures that our social media use aligns with our charitable purposes, protects our reputation, and complies with legal requirements. It draws from Charity Commission guidance on digital media (e.g., CC9 on campaigns, CC26 on risk management, and cyber crime protections against phishing/social engineering) and our Constitution (Article 19, which excludes social media for formal notices, and Article 21 on protecting reputation and assets). Social media activities must not endorse political parties, promote extremism, or breach data protection laws (GDPR). Misuse can lead to reputational harm, legal issues, or serious incident reporting, including scams targeting members via platforms like WhatsApp.

2. Purpose

The purpose of this policy is to:

- Provide clear guidelines for trustees, volunteers, staff, and members on acceptable social media use when representing or associated with UMCUK.
- Ensure social media enhances our charitable objects (Constitution Article 4) while mitigating risks such as misinformation, reputational damage, data breaches, or social engineering scams (e.g., phishing attempts via WhatsApp).
- Promote positive, respectful engagement that reflects our values of unity, diversity, and Islamic principles.
- Outline procedures for content creation, monitoring, and handling issues to maintain transparency and accountability.
- Support compliance with laws and Charity Commission standards for digital communications, including protections against cyber threats like verification code scams.

3. Scope and Definitions

This policy applies to all UMCUK-related social media use, including official accounts, personal accounts when referencing the charity, and activities like events or fundraising. It covers platforms such as X, Facebook, Instagram, WhatsApp groups (for informal communication), and emerging tools.

- **Social Media**: Online platforms for sharing content, including text, images, videos, and interactions (e.g., posts, comments, shares).
- **Official Accounts**: UMCUK-branded profiles managed by authorized personnel.
- **Personal Use**: Individual accounts; users must avoid implying they represent UMCUK unless authorized.
- **Content**: Any post, comment, image, or link shared on social media.
- **Misuse**: Includes abusive language, discrimination, sharing confidential information, or content that harms the charity's reputation, as well as falling for or facilitating scams like social engineering.
- **Social Engineering/Phishing**: Attempts by bad actors to manipulate users (e.g., via fake messages requesting verification codes) to gain access to accounts or sensitive data.
- **Dispute-Related Content:** Any sharing of information about internal conflicts, such as property disputes or governance issues, which could lead to public polarization or GDPR breaches if involving personal/sensitive data.

Exclusions: Formal notices (e.g., AGM announcements) must use email or post (Constitution Article 19).

4. Procedures

Account Management

- Official accounts are created and managed by the General Secretary or designated volunteer (e.g., from the Functions Committee, Article 10(7)). Access is limited to approved users with two-factor authentication (2FA) enabled to prevent hijacking.
- Personal and official accounts must be separated; do not use personal accounts for official posts without approval.
- Passwords and access must be reviewed annually or upon role changes. For WhatsApp groups, enable privacy settings (e.g., admin-only additions) and require explicit consent before adding members.

Content Creation and Posting

- All content must align with UMCUK's purposes, be accurate, respectful, and non-partisan (Constitution Article 2(d)). Avoid political endorsements, hate speech, or sensitive topics without Board approval.
- Approval Process:
    - Routine posts (e.g., event reminders): Reviewed by at least 2 authorized users.
    - Sensitive content (e.g., campaigns): Approved by the Board or Senior Management Team.
- Guidelines:
    - Use inclusive language; respect diversity (Article 4.2(a)).
    - Credit sources; avoid copyright infringement.
    - For images/videos: Obtain consent (e.g., from event attendees); comply with GDPR.
    - Respond to comments professionally; escalate issues promptly.
- Prohibited: Sharing personal data without consent, abusive content, or misinformation. Do not post sensitive/legal documents (e.g., in disputes), as this risks GDPR breaches and exposure to scams. In the event of internal disputes, do not share details on any platform; instead, escalate via the Complaints Policy or Disciplinary Committee (Article 10(1)) to prevent public polarization and maintain confidentiality.

Monitoring and Engagement

- Official accounts are monitored daily by the responsible officer for comments, messages, and risks, including suspicious contacts or scam attempts.
- Respond to queries within 48 hours; positive engagement encouraged.
- Handle negative comments: Acknowledge, investigate if valid, and respond factually. Delete spam/hate speech and block repeat offenders.
- Report serious issues (e.g., threats, extremism) as incidents (Article 15(3)).

Preventing and Responding to Social Engineering/Scams

- **Awareness**: Users must be vigilant against phishing, such as unsolicited messages requesting verification codes, personal info, or links. Never share WhatsApp verification codes—these are for account security only and can lead to hijacking.
- **Prevention Measures**:
    - Enable 2FA on all accounts and advise members to do the same.
    - Verify suspicious contacts (e.g., call to confirm identity).
    - In groups, admins must monitor for spam and remove bad actors promptly.
    - Educate via posts or training: Warn about common scams (e.g., "code requests" to steal accounts or access data).
- **Response**: If a scam is suspected (e.g., a member reports being targeted), immediately warn the group, remove the actor, and report to WhatsApp. If involving data breaches, follow Privacy Policy (notify ICO within 72 hours if high-risk). Log as a potential serious incident for Charity Commission reporting if it affects the charity (e.g., member data exposure).

Crisis Response

- If a post or scam causes harm (e.g., backlash or data leak), remove it immediately, issue a correction/apology if needed, and notify the Board. For dispute-related crises, refer to the Complaints Policy for resolution and avoid further public discussion.
- For data breaches or legal risks, follow Privacy Policy procedures, including GDPR notifications.

5. Responsibilities

- **All Users (Trustees, Volunteers, Members)**: Adhere to guidelines; report misuse or scams (e.g., suspicious messages) immediately; separate personal views (e.g., add disclaimers like "Personal opinion, not UMCUK's"). Never share codes or sensitive data.
- **General Secretary**: Oversee accounts, approve content, monitor compliance, handle escalations, and coordinate scam responses.
- **Treasurer/Finance Sub-Committee**: Assist if involving fundraising ads or costs related to scams (e.g., recovery).
- **Trustees/Board**: Approve policy, review high-risk content, ensure training (including on scams), and address breaches via disciplinary procedures (Article 10(1)).
- **Designated Social Media Leads**: Daily monitoring and posting, with training on risks like phishing.

6. Monitoring and Review

- **Logging**: Track posts, engagements, issues (including scam attempts), and responses in a secure register; review quarterly at Board meetings (Article 8).
- **Annual Review**: The Board assesses effectiveness, trends (e.g., engagement metrics, scam incidents), and updates based on feedback or changes (e.g., new platforms or threats). Include in Annual Report (Article 15).
- **Training**: Provide induction and annual refreshers on this policy for all involved users, with focus on recognizing and preventing scams like verification code phishing and handling dispute-related content.
- **Audits**: Conduct periodic audits of accounts for compliance and security.

7. Related Policies

- This policy links to: Privacy Policy and Terms of Use (data handling, website links), Complaints Policy (escalating unresolved issues), Safeguarding Policy (protecting vulnerable groups online), Risk Management (reputational and cyber risks), and Constitution (Articles 19 on communications, 21 on reputation protection). Breaches may invoke disciplinary actions.

This policy will be reviewed annually or sooner if needed. Amendments require Board approval and Charity Commission notification if material (Article 13). It is available on the UMCUK website and upon request. For questions, contact the General Secretary at info@umcuk.org.

E-mail: info@umcuk.org
75 Derby Road, East Ham, London, E7 8NH
Web: https://umcuk.org/