Internal Risk Management 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) committed to promoting the welfare, culture, religion, education, and health of the Ugandan Muslim community in the UK through volunteer-led activities, events, and outreach. As a small, donation-reliant charity, we face risks such as financial instability, reputational damage from disputes, operational challenges in events, and external threats like social engineering or cyber scams.

This policy ensures proactive identification, assessment, and mitigation of risks to protect our assets, beneficiaries, and reputation. It incorporates recommendations from historical Audits and Investigations (e.g., governance strengthening, financial controls, and due diligence) to prevent recurrence. It complies with Charity Commission guidance (CC26: Charities Reserves and Risk Management), which requires trustees to manage risks responsibly, and our Constitution (Article 4.2(j) on risk management, Article 21 on protecting reputation and assets, and Article 15(3) on serious incident reporting). Effective risk management supports our charitable objects (Article 4) and demonstrates good governance.

2. Purpose

The purpose of this policy is to:

- Establish a systematic approach to identifying, assessing, mitigating, and monitoring risks across all UMCUK activities, including fundraising, events, volunteer management, digital communications, and governance processes.
- Ensure risks are managed in line with our resources and volunteer-led nature, preventing or minimizing harm to beneficiaries, members, assets, or operations, while addressing historical weaknesses like those in the 2025 Arbitration Report (e.g., fragmented authority, procedural breaches, and community mistrust).

- Promote a risk-aware culture among trustees, volunteers, and sub-committees, with clear accountability and reporting, incorporating report recommendations for independent oversight, training, and transparency.
- Facilitate compliance with legal obligations (e.g., Charities Act 2011, GDPR for data risks) and enable timely reporting of serious incidents to the Charity Commission.
- Support strategic decision-making by integrating risk considerations into planning and reviews, turning the 2025 Arbitration report's "transformative opportunity" (Executive Summary) into sustainable practices.

3. Scope and Definitions

This policy applies to all UMCUK trustees, volunteers, staff, sub-committees (e.g., Finance, Functions), and divisional activities (Article 12). It covers all risk categories: financial (e.g., donation shortfalls or unauthorized transfers), operational (e.g., event safety or property management), reputational (e.g., disputes or scams), compliance/legal (e.g., GDPR breaches or Charity Commission non-compliance), and strategic (e.g., partnership failures or governance lapses). It builds on the 2025 Arbitration report's identification of systemic issues (Sections II-III: fragmented structures, weak oversight, historical mistrust).

- **Risk**: Any event or uncertainty that could impact UMCUK's ability to achieve its objectives, positively (opportunities) or negatively (threats), including those from the 2025 Arbitration report like parallel power structures or public polarization.
- **Risk Register**: A documented tool listing risks, their likelihood/impact, mitigation actions, and owners.
- **Likelihood**: Probability of occurrence (low/medium/high).
- **Impact**: Potential severity (low/medium/high, e.g., financial loss, harm to beneficiaries, or community division).
- **Mitigation**: Actions to reduce risk (e.g., controls, insurance, training).
- **Serious Incident**: A risk that materializes causing significant harm, loss, or damage, reportable to the Charity Commission (e.g., fraud, data breach, or governance breaches as in the report).

4. Procedures

Risk Identification

- Risks are identified through: Board meetings (quarterly, Article 8), sub-committee reports (Article 10), annual reviews, incident logs (e.g., from complaints or scams), external audits (if applicable).
- Sources include: Financial reports, event feedback, digital monitoring (e.g., WhatsApp scams), stakeholder input, and post-dispute reviews to capture issues like mistrust or procedural non-compliance.

Risk Assessment

- Use a simple matrix: Score likelihood (1-3) and impact (1-3); total score determines priority (low 1-3, medium 4-6, high 7-9).
- The General Secretary leads assessments, with input from relevant officers (e.g., General Secretary for reputational risks).
- Update the risk register with details: Description, score, potential consequences.

Risk Mitigation

- For each risk, assign actions aligned with report recommendations:
    - High risks (e.g., governance breaches): Immediate controls like independent fact-finding, disciplinary measures, and mandatory training.
    - Medium (e.g., financial oversight lapses): Monitor via consolidated accounts and audits.
    - Low: Accept but review (e.g., minor operational issues).
- Allocate owners (e.g., sub-committee heads) and timelines, with Trustees monitoring compliance.

Reporting and Escalation

- Report new/emerging risks to the Board immediately.
- Serious incidents (e.g., scam leading to data loss or dispute escalation): Notify Commission promptly (Article 15(3)); follow Privacy Policy for GDPR breaches (report to ICO within 72 hours if high-risk). Use report's roadmap for implementation and quarterly progress reports.

5. Responsibilities

- **All Users (Trustees, Volunteers, Members)**: Identify and report risks promptly; follow mitigation actions, including those from the report (e.g., adhering to governance processes).
- **General Secretary**: Maintain the risk register, lead assessments, prepare and coordinate quarterly reports, handle operational/reputational risks (e.g., disputes, scams), and support Trustee oversight.
- **Treasurer**: Integrate and manage financial risks in the report (e.g., unauthorized transfers).
- **Sub-Committees**: Assess risks in their areas (e.g., Functions for events, Finance for funds), incorporating report lessons (e.g., due diligence in procurement).
- **Trustees/Board**: Oversee policy, approve the risk register annually, ensure resources for mitigation (e.g., training), Monitor compliance with mitigations, verify progress on report roadmap, and implement report recommendations like disciplinary measures and independent reviews.

6. Monitoring and Review

- **Logging**: Maintain a central risk register (updated quarterly); log incidents and actions, including those from the report (e.g., governance breaches).
- **Annual Review**: The Board reviews the register and policy at the first post-year-end meeting, incorporating lessons (e.g., from disputes or scams) and report recommendations for institutional strengthening. Include summary in Annual Report (Article 15).
- **Training**: Provide induction and annual sessions on risk awareness (e.g., spotting scams, governance compliance), per report Section VIII.2.5.
- **Audits**: Conduct internal reviews or external if needed (e.g., for high-risk areas like financial controls); use independent fact-finding for unresolved issues (report Section IX.1).

7. Related Policies

- This policy links to: Financial Reserves Policy (financial risks), Complaints Policy (escalation), Safeguarding Policy (vulnerable groups), Social Media Policy (digital risks like scams and disputes), Privacy Policy (data breaches), and Constitution (Articles 4.2(j) on risks, 21 on assets). Breaches may invoke disciplinary actions (Article 10(1)).

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 Treasurer.