Risk Management Policy

1. Purpose and Aim

This policy establishes Coempowered's approach to identifying, assessing, and mitigating risks, particularly those related to online activities. The aim is to ensure the safety, security, and effectiveness of Coempowered's programs while fostering trust among participants, staff, and stakeholders.

By focusing on online risks, this policy recognizes the unique challenges associated with digital platforms and sets clear guidelines to minimize potential harm or disruptions.

2. Scope

This policy applies to:

- All online programs, sessions, and communications facilitated by Coempowered.
- All staff, volunteers, participants, and external partners using Coempowered's digital platforms.
- Tools and platforms such as video conferencing, learning management systems, and communication apps like Telegram.

3. Key Principles

1. **Proactive Risk Identification**:
    a. Risks are identified and assessed regularly to prevent issues before they arise.
2. **Participant and Data Safety**:
    a. Safeguarding participants and ensuring the confidentiality of their data are central to risk management efforts.
3. **Transparency**:
    a. All stakeholders are informed about risks and the measures in place to address them.
4. **Continuous Improvement**:

    a. Regular evaluation and updates ensure that risk management practices evolve with technological changes and emerging threats.

4. Procedures

4.1 Identifying Risks

1. **Categories of Online Risks**:
    a. **Cybersecurity Threats**: Hacking, phishing, or unauthorized access to platforms.
    b. **Data Breaches**: Accidental or intentional exposure of sensitive participant information.
    c. **Inappropriate Content**: Sharing or exposure to harmful or unsuitable materials.
    d. **Online Harassment**: Bullying, grooming, or other harmful interactions among participants or staff.
    e. **Technical Disruptions**: Loss of access, poor connectivity, or platform failures.
2. **Risk Assessments**:
    a. Conduct routine risk assessments for all online platforms and activities.
    b. Identify potential vulnerabilities, such as outdated software or poorly configured privacy settings.

4.2 Mitigating Risks

1. **Cybersecurity Measures**:
    a. Use secure, password-protected platforms for all online activities.
    b. Ensure regular updates and maintenance of software and tools.
    c. Implement two-factor authentication (2FA) for staff and volunteers where appropriate.
2. **Data Protection**:
    a. Limit access to participant data based on roles and responsibilities.
    b. Encrypt sensitive information and back up data securely.
3. **Behavioral Safeguards**:
    a. Enforce the Code of Conduct to prevent harassment, bullying, or inappropriate behavior.
    b. Monitor sessions to ensure compliance with guidelines.
4. **Content Moderation**:

    a. Approve all shared content and resources before dissemination.
    b. Use content filters or moderators for platforms like Telegram.

5. **Contingency Planning**:
    a. Establish backup plans for technical disruptions, such as alternate platforms or recorded materials for missed sessions.

4.3 Incident Response

1. **Immediate Action**:
    a. Address online risks as they arise, such as removing harmful content or blocking malicious users.
    b. Notify the line manager for further action.
2. **Documentation**:
    a. Record all incidents, including their nature, actions taken, and outcomes.
3. **Follow-Up**:
    a. Investigate incidents thoroughly to identify root causes and prevent recurrence.

5. Responsibilities

1. **Staff and Volunteers**:
    a. Follow risk management procedures and report potential risks promptly.
2. **Responsible Person**:
    a. Lead risk assessments and oversee mitigation efforts.
    b. Provide training and support to staff and volunteers on online risk management.
3. **Leadership Team**:
    a. Review risk management practices and allocate resources for effective implementation.

6. Monitoring and Evaluation

1. **Ongoing Monitoring**:
    a. Continuously monitor online activities and platforms for emerging risks.
2. **Regular Reviews**:
    a. Conduct quarterly reviews of risk management practices.

    b. Update policies and procedures based on new threats or technological advancements.

7. Training and Awareness

1. **Staff and Volunteers**:
    a. Receive regular training on online risk management, data protection, and incident response.
2. **Participants**:
    a. Provide age-appropriate guidance on staying safe online, such as avoiding phishing scams or sharing personal information.

8. Compliance and Legal Framework

This policy adheres to relevant data protection regulations and online safety laws, including:

- General Data Protection Regulation (GDPR).
- National and local cybersecurity guidelines.

9. Contact Details

Responsible officer:
Name: [Insert Name]
Contact: [Insert Email/Phone]

10. Review and Updates

This policy will be reviewed annually or in response to significant technological or operational changes to ensure continued effectiveness and relevance.