Lively Minds External Cyber Bullying Policy

Policy owner: Head of HR
Approved by: CEO and COO
Launch date: June 2025
Next review date: June 2026

1. Introduction

Values and Principles

At Lively Minds, we are committed to fostering a culture of respect and digital responsibility in all our interactions, whether internal or external, physical or virtual. Our guiding values include:

a. Taking responsibility for our actions and encouraging ethical and responsible online conduct.
b. Protecting individuals from the psychological harm caused by cyberbullying.
c. Ensuring our digital platforms are welcoming and free of hate, harassment or bias.
d. Addressing incidents swiftly, consistently and in a procedurally fair manner.

2. Purpose of the Policy

Why the need for this policy

Lively Minds maintains a zero-tolerance stance on all forms of bullying and harassment including those carried out through technology, digital platforms or social media.

This policy aims to prevent and address all forms of external cyberbullying involving our organisation including but not limited to interactions with our clients, partners, beneficiaries, vendors and members of the public on social media, emails, messaging apps and other digital platforms.

This policy also protects staff and stakeholders who are subjected to cyberbullying as a result of their association with Lively Minds.

3. Objectives of the Policy

What we want to achieve with this policy

The objectives of this policy are to:

a. define external cyberbullying and reinforce our zero-tolerance stance.
b. outline procedures for reporting, investigating and responding to such incidents.
c. safeguard staff, volunteers, contractors, temporary staff, partners and other stakeholders associated with Lively Minds from reputational and psychological harm.
d. Foster an ethical digital culture that reflects our values and complies with national and international standards.

4. Scope of the Policy

Who the policy applies to

This policy applies to:

a. all individuals interacting with our organisation including clients, community members, partners, donors and followers on social media.
b. All staff, contractors, Board members, temporary staff and volunteers who are targeted online in relation to their roles at Lively Minds.
c. All digital channels associated with our operations including email, social media, websites, messaging platforms like WhatsApp as well as virtual workspaces.

This policy applies regardless of location, whether communication is cross-boarder or domestic and includes content shared anonymously or via third part channels.

5. Definitions

Glossary of terms

5.1 Cyberbullying: Bullying that takes place over digital devices like mobile phones, computers, and tablets. It can occur through SMS, text, and apps; or online in social media, forums, or gaming where people can view, participate in, or share content. Cyberbullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation. - Source: UNESCO

Examples of cyberbullying include:

- Spreading false information, defamatory gossip, or lies about someone online.
- Posting or sharing embarrassing photos or videos on social media without consent.
- Sending abusive, threatening, or hurtful messages, images, or videos via messaging platforms.
- Trolling (i.e. when someone posts deliberately offensive or provocative online content to upset or harass others) - Source: UNICEF
- Cyberstalking (i.e. when someone online repeatedly follow, monitor or harass another person to cause fear, emotional distress or anxiety).
- Impersonating someone online to mislead or cause harm.
- Doxing (publishing private or personal information without consent).
- Engaging in hate speech or discriminatory remarks.
- Using generative AI tools to create or distribute harmful content, including harassment or manipulation

While cyberbullying may occur alongside face-to-face bullying, it differs in that it leaves a digital footprint, a traceable record that can be used as evidence to report and stop the abuse (source - UNICEF).

5.2 External actor: anyone not employed or contracted by the organisation but who interacts with or affects the organisation through online platforms. This includes former staff including temporary staff, former contractors, former volunteers, clients, the general public, vendors, community members, anonymous users etc.

5.3 Target: A person associated with the organisation who is the subject of cyberbullying.

6. Policy Statement

Our declaration

Lively Minds will not tolerate cyberbullying or any form of online harassment directed at our staff, volunteers, contractors, temporary staff, Board members, any person(s) affiliated to the organisation or on our organisational platforms. We reserve the right to report, restrict, block or take legal action against individuals or groups who engage in such behaviours or actions.

7. Procedure

The step by step process

7.1 Reporting

When you experienced or are a target of any form of cyberbullying, immediately report the incident by taking the following actions:

a. Keep evidence of cyberbullying. Screenshot and save all messages received. Use this evidence to report cyberbullying to:
   - The dedicated email address - cybersafety@livelyminds.org or
   - Complete the digital cyberbullying report form at Lively Minds website (add the link) or
   - Escalate to Line Manager or Head of HR if cyberbullying involves internal staff to staff cyberbullying.
   - Line Manager to escalate reported online harassment or abuse to Head of HR.

b. When sharing information via email, make sure to include the following:
   - Screenshots of evidence and/or URLs
   - Share personal information (optional)
   - Summary of incidents including date(s) and time(s) incidents happened.
   - Indicate if you want to be contacted or need any support.
   - Indicate platform used
   - Indicate country where the incident happened
   - Details of the identity of the perpetrator (if known)

7.2 Investigation

The Cyberbullying Response Team (CRT) will:

a. Acknowledge receipt of the report within 48 hours.
b. Assess the credibility and severity of the claim including reviewing the evidence sent.
c. Investigate and collect further evidence (metadata).
d. Consultation with national cybercrime units (e.g. CSA Ghana, UCC Uganda or UK police) per the jurisdiction of where the incident occurred.

7.3 Response Measures

If the perpetrator is eventually identified, the following actions may be taken by Lively minds:

a. Block/remove offender from organisational digital platforms.
b. Ban from attending virtual events, webinars etc.
c. Report to platform administrators e.g. WhatsApp, LinkedIn, X, Zoom etc.
d. Where the incident violates national or international law e.g. cyberstalking, threats, defamation, sexual harassments etc, the case may be referred to:
    - Cyber Security Authority (Ghana)
    - Uganda Policy Cybercrime Unit or UCC
    - UK Police or National Cyber Crime Unit (NCCU) or
    - The Cybercrime Unit of the country where incident happened.

This may include Lively Minds submitting digital evidence, filing a report or cooperating in an official investigation.

e. Pursue civil or criminal action as permitted by national law.
f. Where the offender is an external partner, funder or service provider:
    - The organisation will formally terminate the working relationship or engagement.
    - A cease-and-desist notice may be issued.
    - Communications may be restricted to designated staff or via legal channels only.

    This measure is taken to protect the wellbeing of staff and uphold organisational integrity, even when it affects business continuity or funding streams.

7.4 Support and Recovery

a. Lively Minds will offer mental health support or counselling services depending on country availability to the affected person.
b. Ongoing monitoring and wellbeing check ins.
c. Identity protection guidance.

7.4 Cyberbullying Response Team (CRT)

a. The CRT shall be made up of:
    - COO
    - Head of HR
    - Country Director
    - Global IT Manager

a. The role of the CRT
    - Analyse the report to determine the urgency, credibility, level of risk to the individual and/or organisation and appropriate handling of the incident.
    - Coordinate investigation including collecting evidence, interviewing relevant parties where appropriate and ensure objectivity and protection of all involved.

- Submit a comprehensive investigation report to the CEO outlining findings, actions taken and recommended next steps.
- Lead in the implementation of response actions including policy update and training based on findings.
- Maintain confidential records of all incidents and outcomes.

8. Guidelines

What to do when Experiencing Cyberbullying

Steps to take when dealing with cyberbullying:

8.1 **Do not reply or engage** – When you experience cyberbullying, it is important you avoid replying to the abusive or hurtful messages. It can escalate the situation.

8.2 **Take screenshots** – Do not delete any of the abuse you receive online. Capture and save all evidence:

- screenshots of offensive messages, posts & images (make sure they have the timestamps and dates)
- profile information of the abuser including username or profile details if they use anonymous accounts
- chats or message logs (export or copy full conversations where possible).
- emails including full headers if available
- URLs or links (direct links to posts, profiles or contents related to the abuse)
- voicemails or audio messages
- videos
- platform reports made etc.

8.3 **Block the bully** – Make sure to block the bully from the relevant social media platform to avoid the Bully from contacting you or seeing your content. Avoid accepting friendship requests from unknown people for a while as the Bully may try to use another fake account to contact you.

8.4 **Report the abuse** – Report the abuse via the email address provided – cybersafety@livelyminds.org or complete the online report form. This is an important step to help initiate an investigation into the incident.

8.6 **Do not share the abusive content further** – Avoid forwarding or reposting the harmful content to others.

8.7 **Get support** – Ask for emotional or mental health support if you are feeling anxious, stressed or unsafe.

8.9 **Follow up** – Follow up on the status of the investigations and actions taken. If unsatisfied with the outcome, express your concerns or report to the local police or a cybercrime unit.

Guidelines to Stakeholders

All external actors engaging with the organisation must:

a. Treat organisational representatives with respect and dignity online.
b. Refrain from online harassment, abuse, defamation, threats or cyberstalking.
c. Do not use or share digital content involving staff or brand materials without consent.
d. Understand that such actions may lead to legal consequences and/or severance of organisational ties.

10. Legal and Regulatory Context

This policy aligns with the following laws and frameworks:

Ghana

- Cybersecurity Act, 2020 (Act 1038) – Prohibits electronic communication that causes harm or distress.
- Electronic Communications Act, 2008 (Act 775)
- Enforced by the Cyber Security Authority (CSA) and Ghana Police Cyber Crime Unit.

Uganda

- Computer Misuse (Amendment) Act, 2022 – Criminalises sending messages without consent or likely to ridicule or degrade another.
- Uganda Communications Commission (UCC) Guidelines.
- National framework on online protection, especially for women and children.

United Kingdom

- Online Safety Act 2023 – Establishes a duty of care for platforms to prevent harm from illegal and harmful content.
- Malicious Communications Act 1988, Protection from Harassment Act 1997, and Defamation Act 2013

Enforced by Ofcom, UK Police, and civil courts.

International Instruments

- UNCRC, UNESCO Digital Literacy Guidelines, OECD Guidelines, EU GDPR, African Union Convention on Cybersecurity and Personal Data Protection.

9. Communication and Acceptance

a. This policy shall be hosted on our website and shared with staff, partners and the public.
b. Stakeholders shall be deemed to have accepted the policy by interacting on our digital platforms, personnel and affiliates.
c. Contractors, collaborators and donors shall confirm acceptance to comply with our policy by signing a Cyberbullying Non-Engagement Declaration Form (Annex A).

10. Responsibilities

	Role	**Responsibility**
1.	Board	Policy oversight and risk governance.
2.	CEO	- Receive, review and oversee the implementation of recommendations from the comprehensive investigation report submitted by the CRT. - Approve engagement with legal counsel or external investigators when deemed necessary. - Escalate serious or high risk cases to the Board as appropriate.
3.	COO	- A member of the CRT. - Work closely with the CEO by ensuring operational implementation of the Cyberbullying Policy across all countries and supporting compliance.
4.	Country Directors	- Members of the CRT. - Escalate incidents of cyberbullying brought to their attention to the CRT. - Leads incident reporting to the appropriate law enforcement agency at the national level. - Ensure in-country collaborators with Lively Minds at the national level sign the Cyberbullying Non-Engagement Form. - Sign the Cyberbullying Desistance Declaration Form as the representative of Lively Minds.

5.	HR	- A member of the CRT. - Ensure reported incidents are duly acknowledged within the stipulated deadline. - Escalate received incidents appropriately. - Coordinate access to emotional and mental health support to affected person where required. - Ensure regular policy review to reflect evolving digital risks and incorporate lessons learnt from investigated cases. - Coordinate with IT to ensure regular training, refresher sessions, and orientation are provided to all staff to promote awareness and compliance with the External Cyberbullying Policy.
6.	IT	- A member of the CRT. - Monitor Lively Minds digital platforms to ensure adherence to the External Cyberbullying Policy. - Share updates on evolving digital risks and emerging technologies to inform staff training in collaboration with HR.
7.	Line Manager	Report concerns brought to their attention promptly to the key contact of the CRT.
8.	Staff and Lively Minds affiliates	Report concerns promptly to the appropriate channels and refrain from retaliating online or reporting to others.
9.	Legal Advisor (Internal or External)	- Provided legal counsel - Leads legal action - Ensures lawful responses per national frameworks.

11. Training

Training on this policy will be conducted annually as part of the organisation's safeguarding programme to reinforce staff responsibilities and keep pace with emerging digital risks. It will also be integrated into the induction programme for all new joiners to ensure early awareness.

13. Review of the Policy

This policy shall be reviewed annually or as needed in response to changes in relevant laws, emerging digital risks or after any significant incident involving online abuse.