

How to.... Manage Social Media and Online SOGIESC-Based Harassment

Visible, public support and allyship with LGBTQIA+ communities is not optional for humanitarian organisations committed to inclusion and the humanitarian principles - it is a core expression of that commitment. Self-censoring SOGIESC content, quietly removing Pride posts, scrubbing websites, or avoiding public statements on inclusion....it all sends a powerful message to LGBTQIA+ staff, communities, and partners that the organisation is not committed to LGBTQIA+ inclusion. It sends a message that the organisation's commitment to the LGBTQIA+ community will yield when under pressure.

Social media has always had a volatile side, and it has always suffered from providing access to users espousing hate, discrimination, and violence. This guide focuses on what happens if the organisation itself becomes the target. The document looks at what is within organisational control: how to prepare before harassment occurs, how to respond when it does, and how to protect staff who manage public-facing communications.

- **Preparation is the Best Protection:** Organisations that have planned for online SOGIESC-based hostility respond better, faster, and with less impact to staff and reputation.
- **Do Not Stay Silent:** Failing to respond to public SOGIESC-based hostility is itself a message - that the organisation's values are conditional.
- **Do Not Escalate Carelessly:** Engaging directly with trolls or hostile campaigns can amplify harm. Every response decision should be deliberate, values-led, and coordinated.
- **Protection for Communications Staff:** Staff who manage organisational social media accounts are on the front line of online hostility. Their wellbeing is paramount.
- **Consistency Builds Credibility:** Organisations that respond to SOGIESC-based hostility consistently build genuine trust with LGBTQIA+ communities and allies.

If online hostility toward the organisation includes credible threats of physical violence against named staff members, or if it appears to be part of a coordinated campaign that could endanger staff operating in restrictive legal environments, activate your organisation's security and crisis management protocols immediately.

Practical Steps for Aid Organisations

1. Preparedness

- Develop an online hostility response protocol. This should include: who is authorised to respond on behalf of the organisation; which content requires which response e.g. direct

response, moderation, silence; escalation thresholds; and who must be informed when an incident occurs.

- Identify and train a small, designated response team – such as, Communications Manager, Human Resources or Safeguarding Focal Point, Director - who can be convened quickly when an incident occurs. Define roles and responsibilities.
- Prepare template response statements for various scenarios e.g. a hostile message following a Pride Month post; a disinformation campaign targeting the organisation's SOGIESC work.
- Map the organisation's digital footprint: which platforms are active, who manages each account, and what the escalation path is if account credentials need to be secured quickly.
- Establish a routine monitoring process for the organisation's mentions, tags, and accounts across relevant platforms.
- Review and test this protocol annually. Online hostility tactics evolve rapidly. A protocol written two years ago may not anticipate the forms of attack that are most common today.

2. Social Media Governance

- Define who is authorised to post, respond, and moderate on behalf of the organisation across all platforms.
- Ensure that account credentials are held securely by the organisation - not only by individual staff members. If a communications staff member leaves or is on leave during an incident, the organisation must be able to act without delay.
- Set clear moderation policies for the organisation's social media accounts: what comments will be hidden or removed, what warrants a direct response, and what will be left without engagement.
- Establish a rapid escalation process: staff managing accounts must know exactly who to contact and how quickly. They should never have to manage a coordinated attack alone.
- Apply for NGO or civil society trusted partner status on major platforms where this is available. This can significantly accelerate content review, account recovery.

3. Protect and Support Staff

- Staff who manage the organisation's social media accounts bear a disproportionate burden during online hostility incidents. They are often the first to encounter hostile content, required to make fast decisions under pressure, and exposed to distressing material in the course of their work.
- Ensure communications staff are never be required to manage a coordinated attack alone, respond to personal abuse directed at them through organisational accounts, or make significant strategic decisions without management approval.
- Offer regular wellbeing check-ins for communications staff, not only after significant incidents. Sustained exposure to lower-level hostility accumulates over time and can be harmful.

- Provide communications staff with specific training on recognising and managing online SOGIESC-based hostility, including their own rights if they are personally targeted through their work on organisational accounts.
- Rotate responsibilities for monitoring and moderating hostile content during sustained incidents. No individual should carry this exposure alone for extended periods.

4. Managing the Response

- If false claims about the organisation's work or values are circulating online, assess carefully whether a direct rebuttal or a broader positive communications push is the more effective response. Direct rebuttal can amplify disinformation; a proactive positive narrative can do more to correct the record.
- Prepare factual, accessible content about the organisation's SOGIESC inclusion work - its mandate, its approach, its evidence base, that can be published or shared quickly.
- Alert key stakeholders such as donors, partners, board members, proactively when disinformation is circulating.
- Document disinformation incidents carefully, including the content, its apparent origin, its spread, and the organisation's response.
- Report hostile content, coordinated harassment, and impersonation accounts to platforms using their formal reporting tools.
- If organisational accounts are suspended or restricted as a result of coordinated reporting abuse, have a pre-prepared recovery plan: alternative communication channels, a contact at the platform, and a clear process for disputing the suspension.
- Standing firm on SOGIESC inclusion under pressure is the most effective long-term reputational strategy. Organisations that visibly capitulate to hostility lose the trust of the communities they work with and LGBTQIA+ staff.

Additional Resources

- **The PRIDE Centre:** Templates, legal analysis, and tools for [LGBTQIA+ inclusion](#) in humanitarian settings.

☑ Checklist for Organizing Pride in Restrictive Environments

- [] **Response Protocol in Place:** A written online hostility response protocol exists, is known to relevant staff, and has been reviewed in the last twelve months.
- [] **Response Team Designated:** A small, named response team - Communications Manager, Human Resources or Safeguarding Focal Point, Director is identified and knows their roles.
- [] **Template Statements Prepared:** Pre-approved response statements exist for foreseeable scenarios: disinformation campaigns, donor pressure, and account suspension.
- [] **Account Governance Secure:** Social media account credentials are held securely by the organisation, not only by individual staff members. Access can be managed quickly if needed.
- [] **Monitoring in Place:** A routine monitoring process tracks the organisation's online mentions and accounts, with increased vigilance around known high-risk moments.
- [] **Key Stakeholders Briefed:** Donors, board members, and key partners are briefed before high-risk moments so they are not caught off-guard if hostility escalates to approaches to them.
- [] **Responses are Coordinated:** No public response is issued unilaterally. All significant responses are approved by the designated response team.
- [] **Values Held Under Pressure:** The organisation has a clear leadership position on maintaining SOGIESC inclusion commitments in the face of hostility, and senior leaders can articulate it confidently.
- [] **Disinformation Managed Proactively:** Factual content about the organisation's SOGIESC work is prepared and ready to publish when the organisation's credibility is under attack.
- [] **Communications Staff Protected:** Wellbeing check-ins for communications staff are routine, not only post-incident. Responsibilities for monitoring hostile content are rotated during sustained attacks.
- [] **Evidence Preserved:** Screenshots with timestamps and URLs are taken before any hostile content is reported to platforms or removed.
- [] **Share Resources:** Direct staff to [The PRIDE Centre](#) for information and guidance.

SUPPORTED BY

With the
participation
of



LUSH



Activity supported by the
Canada Fund for Local Initiatives
Activité réalisée avec l'appui du
Fonds canadien d'initiatives locales

Canada

