# The Waitlist

## Before We Can Organise, We Have to Be Safe


**Suggested Citation:**

Iyer, Neema. “The Waitlist: Before We Can Organise, We Have to Be Safe.” Pollicy, June 2026.

## What African feminist organisations told us about digital safety, and where we can go from here

**133**

Applications received

**20**

Countries represented

**55**

Organisations with no prior formal digital safety training

**15**

Organisations we can support with current funding

# We asked and we received

Pollicy is a feminist collective working at the intersection of data, technology, and advocacy across Africa. We have spent years documenting the experiences of African women in online spaces, from everyday women in the markets to human right defenders to political leaders. We have documented the harassment campaigns, the coordinated disinformation and ultimately, the silencing and censorship. We have published the data around the continent, advocated for safer and joyful internet spaces with technology companies and are actively working with legislative systems. We have also been targets ourselves.

So, when we opened a call for African feminist and women's rights organisations to join our digital safety audit and training initiative, we expected interest. We did not expect what came back.

One hundred and thirty-three organisations applied in just under two weeks. They came from 20 countries across East, West, and Southern Africa, from Nairobi and Lagos and Harare, from Mekelle and Garoowe and Blantyre. They wrote in English, French, and Portuguese. They described being hacked, doxxed, impersonated, stalked. They described staff members in hiding, Twitter/X accounts shut down, Facebook pages made private to keep communities safe. They described spending their evenings correcting disinformation instead of doing the work they are meant to do.

**We initially had funding to support just ten, but were able to bump it up to fifteen.**

# A Decade of Reflection

Pollicy's work on technology-facilitated gender-based violence (TFGBV) goes back to 2018, a year after we were founded, when we conducted 300 in-person interviews with women in Kampala to document their digital security knowledge and experiences of online harassment. At the time, that report, Ugandan Women Online, produced in partnership with Internews, was among the first pieces of research in East Africa to put hard numbers to the facts - that cyberbullying, stalking, and non-consensual sharing of private information were widespread, under-reported, and almost entirely unaddressed by law enforcement or platforms. Nearly a quarter of respondents had experienced cyberbullying and most did not know where to report it.

That baseline research shaped much of what followed. In 2020, Alternate Realities, Alternate Internets, co-authored with Bonnita Nyamwire and Sandra Nabulega, went deeper and wider, speaking to women across five sub-Saharan African countries about their online lived experiences. Its main finding showed that repeated exposure to online violence does not just harm women in the moment. It fundamentally changes how they use the internet, which spaces they enter or leave, and how they show up in the world. The internet was reproducing the same structures of oppression that existed offline, often with greater reach and less accountability.

Our Amplified Abuse report tracked online violence against women politicians during Uganda's 2021 general election. Byte Bullies did the same for Kenya in 2022. Across both, it was evident that women who entered public life online were targeted systematically, and the platforms hosting the abuse provided little meaningful recourse. Our research series African Women in Artificial Intelligence examined how AI systems amplify existing biases and create new forms of harm for African women specifically.

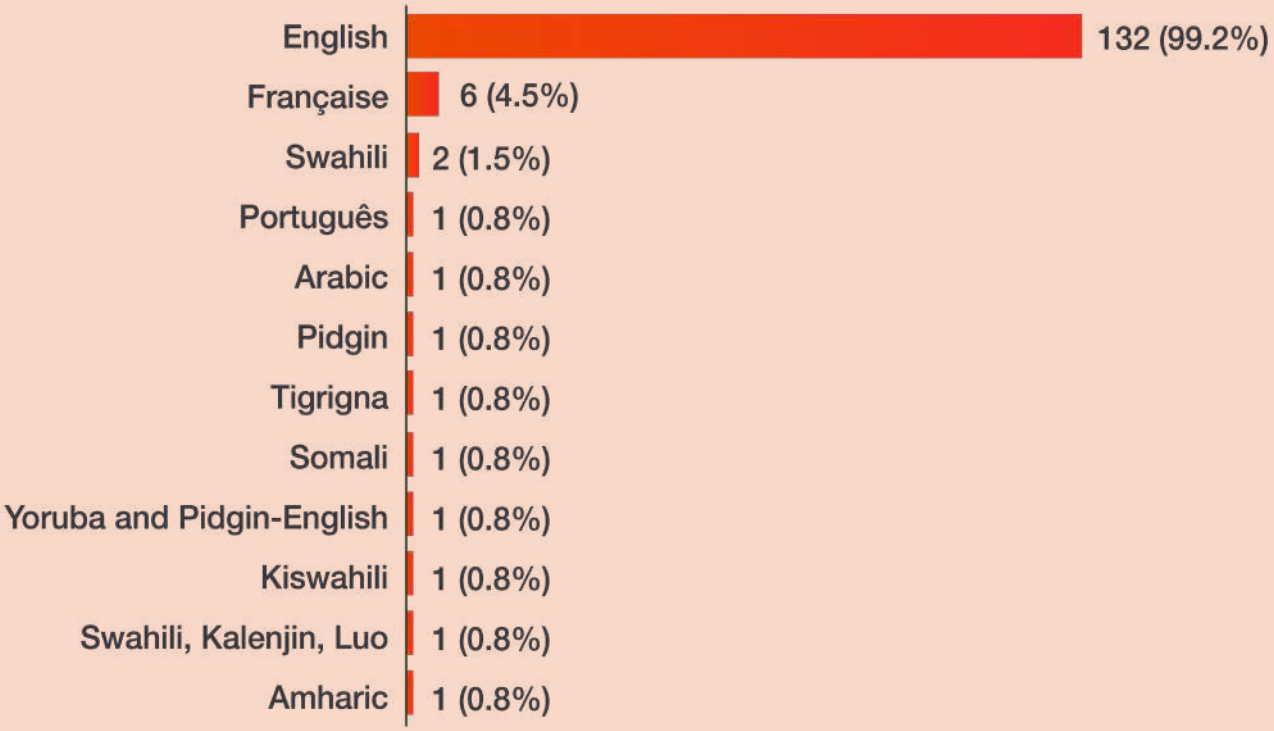
Through all of this, what has remained consistent is that the organisations doing feminist work in digital spaces are themselves under attack and often chronically underprepared to defend themselves because the support infrastructure for grassroots feminist digital safety is drastically underfunded. Most feminist organisations are funded project by project, with every shilling accounted for against a deliverable. There is no budget line for an IT plan, no time set aside for a security audit, no breathing space to ask "are our systems actually safe?" Core and institutional funding remains elusive for most grassroots feminist groups. The result is organisations that are doing vital, high-risk work are keenly aware of the fraying tightrope they are balancing on but are unable to stop long enough to fix it.

Pollicy has not been exempt. Our strategic plan is explicit on this point in our first strategic pillar, that we believe the internet should be a space of connection, creativity, and care. Safety is what makes joy possible. But our third pillar is equally important, it is about strengthening Pollicy as an organisation, so we are better prepared to do the work, to support our peers, and to show up the way we need to. In the past year we have been doing exactly that by bolstering our HR systems, reviewing our policies, and conducting our own internal audits. This very initiative came from us sitting with our own vulnerability, recognising what we lacked, and deciding to build something that addressed that need, both for ourselves and for the wider movement.

# What our Peers Tell Us

## The geography of need

Applications came from 20 countries, namely Uganda, Kenya, Nigeria, Zimbabwe, Zambia, South Africa, Ghana, Rwanda, Ethiopia, Tanzania, Malawi, Namibia, Cameroon, Somalia, Côte d'Ivoire, Sierra Leone, Liberia, Egypt, and Eswatini. Kenya, Nigeria, and Uganda together accounted for the largest share, but the spread across linguistic corridors, i.e. Anglophone, Francophone, Lusophone, reflected the cross-regional reach the programme intended.




The organisations were diverse in their mandates including SRHR collectives working with survivors of sexual violence; LGBTQ+ organisations operating in criminalising legal environments; climate justice movements using digital tools for community storytelling; women journalists; electoral accountability groups preparing for the 2026 and 2027 election cycles in Zambia, Kenya, and Zimbabwe and high-risk shelters and safehouses. Our previous work has made it clear that digital safety can't be relegated to the realm of IT support, but must be understood as the condition under which all of this work either continues or stops.

## What Collective Resilience Actually Means

When we asked applicants what digital safety and collective resilience meant in their own organising, the answers pushed back against any framing of feminist organisations as simply passive targets waiting to be helped. Applicants put it plainly:

> **Collective resilience refers to the fact that we are not struggling with these challenges on our own. We develop secure systems, stand by each other, exchange information, and build trusted networks in order to ensure that our employees, associates, and societies can go on with their activism and leadership without fear and apprehension.**

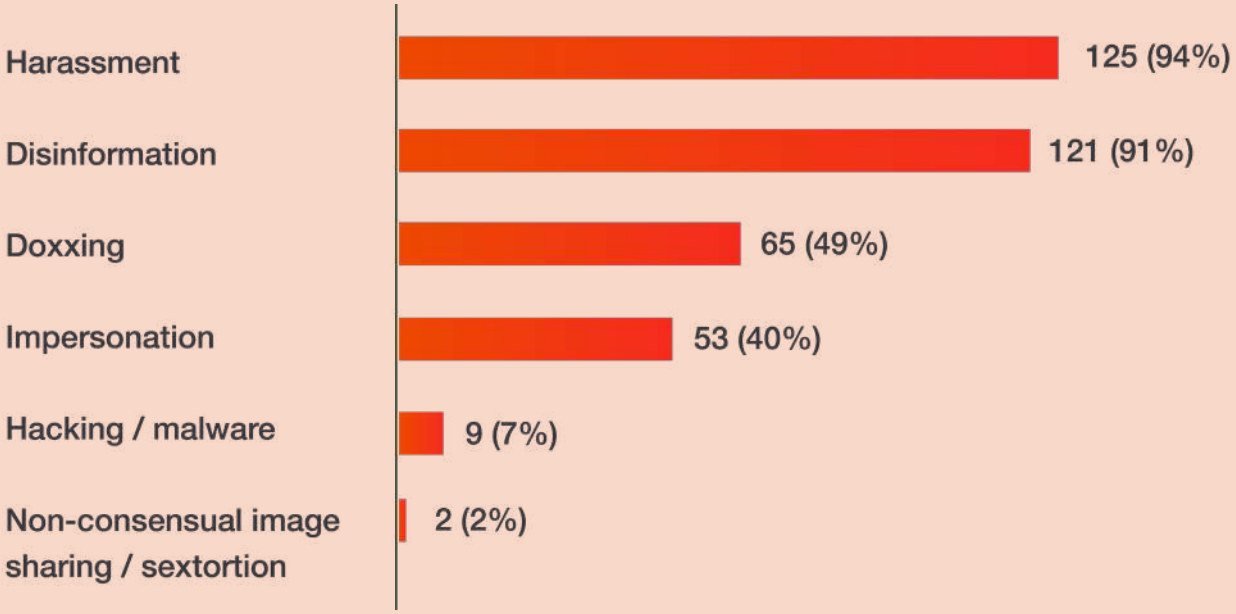
> **For us, feminist digital safety and collective resilience mean ensuring that women and feminist movements can organize, speak, and lead online without fear, violence, or silencing. It is about shared learning, mutual care, and cross-regional solidarity that strengthens feminist power and protects those most at risk in digital spaces.**

**Collective resilience goes beyond individual protection; it is about strengthening our networks, sharing knowledge, and supporting each other so that threats to one do not weaken the movement as a whole. It also involves setting up systems for collective healing in case of a threat and digital harms. Together, these principles ensure that our work can continue safely, boldly, and sustainably, amplifying feminist voices across communities.**

Feminist movements across Africa are already sustaining these practices without external support through building networks, sharing knowledge, holding each other accountable. Holistic digital safety education is well placed to build on the existing infrastructure within organisations. As a feminist collective ourselves, this resonates deeply with Pollicy's own journey of strengthening our internal systems while showing up for others doing the same work.

## The threats they are facing

Harassment was the most commonly reported threat, cited by organisations from every country that applied. Disinformation came a close second. Doxxing, impersonation, and coordinated trolling followed next. Several organisations reported hacking of accounts and websites; others described phishing, ransomware, surveillance of mobile phones, and threats that had escalated from online abuse into physical danger.




A feminist SRHR platform described moralistic disinformation campaigns accusing them of distributing unsafe products with attacks designed to destroy trust and silence an organisation that gives young women access to sexual health information. An organisation running one of their country's primary helplines for domestic violence survivors had their accounts impersonated and vulnerable survivors seeking help were reaching fake accounts instead.

> **The surge in TFGBV fosters Digital Exile, a culture of fear. In Kericho, a large proportion of vulnerable youth, women and PWDs lack the skills to report digital crimes like doxxing or harassment, silencing feminist voices and shrinking civic space.**

> **We basically have to go into hiding most of the time and this limits our work and productivity rate.**

> **It has made us have to scale down our work and extremely close off our spaces which have served as safe spaces for a long time. Misinformation has cost us key government and CSO partnerships.**

The cumulative toll of these attacks impact finances, ability to show up, to do the work, the sense of psychological safety. Multiple applications described staff burnout, anxiety, secondary trauma, and the exhaustion of constant vigilance. Organisations described team members self-censoring, survivors hesitating to share testimonies, community members withdrawing from visibility after watching colleagues get targeted. Overall, it seems that the attacks are working as intended to pull back the gains that the women's right movement has made across Africa and the world more broadly.

## The training gap

Fifty-five (41%) of the 133 organisations reported having received no prior formal digital safety or organisational resilience training. Of those who had received some training, many described sessions that were short, one-off, individually focused, and not tailored to feminist organisational contexts. Several noted that previous training had covered basic device hygiene but not the specific threats their organisations faced such as coordinated harassment, data breaches involving survivor information or sustained disinformation campaigns that worked to destroy community trust.

> **Our current digital safety relies on self-taught methods and open-source research. Despite developing content for others, we lack a professional audit to stress-test our internal systems. We need the structural rigour this programme offers.**

> **We have not yet participated in formal digital safety, safeguarding, or organisational resilience trainings, which makes this programme especially timely and valuable.**

Several organisations described receiving digital safety components as a brief add-on within broader capacity-building programmes which seem enough to give tools to name the risks, not enough to address them. These organisations need an audit, a tailored security plan, incident response protocols, and the organisational infrastructure to sustain safe digital practice over time.

## The urgency is now

Many organisations framed their applications with explicit reference to political timing. Kenya will go to elections in 2027, Zimbabwe in 2028 and Zambia is already in an election year. Many of us are already aware of the cancellation in Lusaka of RightsCon 2026, our main avenue for connecting on global digital rights, signalling a firm closure of civic spaces and the type of work that we do. Multiple applications noted that digital threats intensify around elections whereby anti-rights movements coordinate their attacks, that civic space shrinks fast, and that feminist organisations need to be prepared before the window closes.

> **2026 being an election year poses a huge threat to CSOs and more so grassroots feminist movements in our bid to spread civic awareness. We understand that we will be a target, especially with our past. With the new cybersecurity act the government is using it to shrink civic space.**

Anti-rights movements came up repeatedly across applications. Organisations in Kenya, Uganda, Nigeria, Zambia, and Zimbabwe described coordinated online campaigns originating in anti-LGBTQ+ mobilisation, anti-abortion activism, and political hostility to feminist organising. These are strategic efforts to push feminist voices out of public digital life and they are growing more sophisticated, better resourced, and increasingly transnational.

## How we Selected

With far more applications than places, the selection process proved to be difficult for our team. We assessed each application against four questions: how severe and immediate were the digital threats the organisation faced? How sensitive were the communities and data they were responsible for protecting? How limited was their current digital security capacity? And how likely were they to carry what they learned back into their wider networks?

We gave particular weight to organisations working in the highest-risk environments such as those supporting survivors of violence, defending human rights in criminalising contexts, or operating where civic space is actively shrinking. These are the organisations for whom a security failure is much more than an inconvenience, more likely verging on crisis.

The final fifteen were also selected to reflect the breadth of feminist organising across Africa. They were diverse in geography, thematic focus, organisational size, and language, with deliberate attention to representation across different linguistic contexts. In addition to immediate security needs, we placed significant weight on each organization's readiness to engage in the audit and training process and its potential to share knowledge and strengthen digital safety practices within broader feminist movements and communities.

## Fifteen Organisations, Over a Hundred on the Waitlist

We offer something that we deem different from a standard digital safety training. Each selected organisation receives a full SAFETAG audit which includes an in-depth assessment of their digital infrastructure, identifying specific vulnerabilities and producing actionable, tailored recommendations. They then join a Training-of-Trainers cohort designed around feminist facilitation principles, trauma-informed approaches, and multilingual accessibility. Cross-regional exchanges allow cohort members to share strategies, tools, and solidarity across linguistic and geographic borders.

The program is designed to move organisations from reactive crisis management to proactive, institutionalised digital safety. It takes seriously the fact that feminist organisations are not generic civil society actors but instead they face gendered, targeted, and coordinated forms of digital harm that generic cybersecurity training does not address.

We were able to select fifteen organisations.

The other 118 are still waiting. Some of them described situations that were urgent when they wrote to us. Some of them will be operating in election environments before this programme cycle ends. Some of them are doing work with trafficking survivors, with LBQ women in criminalising contexts, with grassroots communities in fragile political environments where a data breach or a successful impersonation campaign could cause serious harm to real people.

The gap between what is needed and what current funding can provide is a structural failure of the feminist technology funding ecosystem.

## What Needs to Change

Reading all these applications gave us clarity about what is and is not working in the current landscape of digital safety support for feminist organisations. A few things stand out that we would like to make note of.

1. Most available training is one-off and individual in focus. Organisations repeatedly described attending a single workshop that gave them awareness of risks without giving them the tools to address them. A one-day training on phishing does not produce a safeguarding protocol. A short session on secure messaging does not result in an incident response plan. Feminist organisations need sustained, systems-level support, rather than episodic skill-transfer.

2. Safeguarding and digital security are routinely treated as separate concerns, when the applications make clear they are deeply intertwined. An organisation managing survivor data requires both a technical response and a political analysis of what that data means and who may try to access it.

3. Language and geography continue to be excluded. The majority of digital safety resources are in English, and the majority of training infrastructure is concentrated in Anglophone East Africa. Francophone and Lusophone organisations, and organisations in smaller or more remote contexts, are systematically underserved. Several applicants explicitly noted this as a barrier they had already encountered.

4. What feminist organisations need are not more workshops. They need organisational audits, tailored security plans, and the internal infrastructure to maintain safe digital practice over time. They need to be treated as the high-risk, high-value actors they are. The investment required to protect that work is proportionate to its importance.