

Policy Review on Cyberbullying

Nozipho Mojapelo

Zimbabwe Psychology Association

DOI: <https://doi.org/10.47772/IJRISS.2026.100600921>

Received: 20 June 2025; Accepted: 25 June 2026; Published: 08 July 2026

EXECUTIVE SUMMARY

In today's world, community is no longer defined solely by geography, it's defined by connection. In Zimbabwe the digital expansion has caused a severe public health and human crisis. Harassment in the digital era reveals a 75% of students reported having intimidating. The Zimbabwean government enacted the **Cyber and Data Protection Act** [Chapter 12:07] and the **National Child Online Protection Policy** (2026 – 2030 to protect its citizen in the digital era. Studies have highlighted the impact cyberbullying has on the victim's mental health, self-esteem and academic performance. This paper reviews the Zimbabwe's policy and proposes recommendations to help mitigate cyberbullying in communities. Our sense of belonging plays a huge role in mental and emotional wellbeing. That is why using community psychology principles of prevention, empowerment and ecological perspective can help build healthy communities where digital misuse is lessened.

INTRODUCTION

Every second, someone is connecting with another human being in ways our ancestors could have never imagined using what we call internet. We work, fall in love, build communities and share our deepest vulnerabilities through sleek glass screens. Yet underneath this unique era of connectivity lies a dark, pervasive surge that impends the digital society; cyberbullying.

Once confined to schools or workplaces, harassment voyage online, changing into relentless weapon. Cyberbullying is no longer just occasional irritation, it is a profound public health and human rights crisis. Now times have changed as our lives are intertwined with the digital world, such that logging off is no longer a practical. When the abuse gets you the psychological toll becomes inescapable.

To confront this crisis, we must understand what it looks like. Cyberbullying is defined as the intentional, repeated and hostile use of digital communication technologies to harass, exploit, intimidate or humiliate a specific individual or group (POTRAZ, 2023). It is not just "online drama" but a form of interpersonal trauma that demolishes an individual's psychological safety. Mawere (2023) stipulates that cyberbullying manifests as trolling, harassment, cyber stalking or non-consensual image sharing. Unlike traditional bullying, digital harassment results in a permanent, public footprint that the victim cannot evade, interrupting their essential social ecosystems including-family, school and workplace. Psychologists explain that perpetrators feel sense of invisibility due to absence of communication cues such as eye contact and body language. They point out to a phenomenon known as the *Online Disinhibition Effect* (Chikamba & Zhou 2023). These perpetrators hide behind perceived anonymity allowing them to do things online that they would have never carried out face-to-face. Across the globe, over one-third of youth report being cyberbullied but this is not exclusively a youth concern as adults also face this problem. According to Mawere (2023) a survey conducted across Higher and Tertiary Education institutions in Zimbabwe, highlighted that 75% of undergraduates respondents received intimidating messages while on campus. Studies further purports that cyber threats often overlap with sexual and gender based harassment, where power dynamics expose students to predatory behaviour. Another study indicated that 83% of students confirmed encountering explicit, offensive or defamatory messages targeting themselves or peer while engaging on social media platforms. These hostile digital environments have shown to severely affect the students' mental health, self-esteem and academic performance. Furthermore, cyberbullying has direct link to spiral rates of clinical depression, anxiety and suicidal ideation. This policy review paper reviews the policy and proposes recommendations to alleviate cyber bullying.

Current Policy

The government of Zimbabwe established multi-layered policy framework, to protect its citizens. These legal frameworks include the **Cyber and Data Protection Act** [Chapter 12:07] and the **National Child Online Protection Policy** (2026 – 2030) which approach cyberbullying as a series of distinct criminal fractions (Government, 2021)

Cyber and Data Protection Act [Chapter 12:07]

The policy was enacted in December 2021, to govern data privacy and regulating digital offenses in Zimbabwe. It provides a legal foundation devised to safeguard citizens' personal information, penalize cybercrimes, and align the country's technology sector with international standards. To understand why the digital world remains unsafe despite strict statutory interventions, we must analyse the through a psychological lens.

However, Chikamba & Zhou (2023) purports that psychology views cyberbullying as a complex web of behavioural conditioning, cognitive distortions and trauma loops that sustain both aggression of the perpetrator and the emotional distress of the victim. This digital phenomenon produces unique challenges that include psychological vulnerabilities, severe resource constraints, and a critical shortage of specialized skills compared to traditional, in-person bullying.

Challenges

The psychology of Cyberbullying

The frame works surrounding online harassment works on three psychological pillars:

Behavioural Conditioning: This explains how aggressive online behaviour is shaped by reinforcement and social learning.

- Positive reinforcement - The perpetrators are often rewarded through peer validation such as likes or retweets at the expense of another person.
- Observational learning - The social learning theory purports that people imitate aggressive behaviour they normally observe from public figures or pervasive "cancel culture".

Cognitive Distortions: Online environments alter how individuals process information and interactions.

- Disinhibition Effect- The lack of cues such as eye contact, body language or auditory leads to disconnection from moral gravity of one's actions, making it easy to target the victim with no remorse.

Trauma loop: The endless, pervasive nature of the internet turns harassment into psychological distress. This is because digital content is instantly shared and circulates that digital footprint, it creates ever ending cycle of humiliation which takes a psychological toll on the individual. Victims often experience intense emotional distress that manifests as:

- Anxiety and depression: Persistent worry about the being targeted and exposed can trigger clinical depression and panic attacks.
- Trauma: The intrusive thoughts and altered sleep patterns cause the victims to struggle to cope with the loss of their privacy.
- Internalize stigma and shame: The online attacks erode self-esteem which lead to profound social withdrawal and loneliness.
- Self-harm and suicidal Ideation: In extreme cases, the sense of hopelessness and lack of safe escape can tragically lead to self-harm or suicidal thoughts.

Resource Constrains

Despite progressive frameworks such as National ICT Policy and recent AI strategies, resource constraints act as a major bottleneck to progress. The inadequacy for budget allocation and high infrastructure costs severely limit Zimbabwe's capability to deploy advanced technologies and secure institutions like the National Cybersecurity Centre.

Severe skills shortage

While Zimbabwe performs well in Southern Africa for cyber threat mitigation, broader posture is heavily limited by institutional and skill shortages.

Talent Drain: Local security professionals often immigrate to other countries in search for greener pastures which leaves the local enterprises with an acute shortage of analysts. The migration of these professionals leaves unfilled positions causing the public and private organizations dangerously exposed to digital crimes.

Low digital literacy

A sizable fraction of the population lacks awareness of basic digital hygiene, creating a highly vulnerable environment for identity theft and phishing scams. Several users struggle to differentiate genuine messages from manipulative, AI-engineered attacks that sound and look precisely like trusted organizations.

With that said, evaluating Zimbabwe's existing laws uncovers why purely punitive, reactive legal codes fail to stop digital harm. Below are the policy gaps presented on several specific issues;

Irreversible Harm Velocity

The law authorizes the POTRAZ to investigate and prosecute offenders after criminalizing actions such as cyberbullying or non-consensual sharing has occurred. However, when something goes viral it means by the time a criminal investigation is initiated the victim at that time would have already suffered significant emotional distress or reputational damage.

Psychological trauma

A number of studies highlight that digital victimization often leads to chronic psychological harm such as anxiety and depression (ASWN, 2022). This is because online harassment is perpetual causing the victim to struggle with internal shame leading to psychological distress. This harm frequently manifests as social withdrawal, absenteeism or self-harm. The law punishes the perpetrator but it fails to heal psychological scars of the victim.

Underreporting

Statically, only 12% of digital violence victims in Zimbabwe formally report the abuse to law enforcement or POTRAZ (Chakamba and Zhou, 2023). Most victims that encounter digital violation are embarrassed to report and seek assistance which can be due to lack of knowledge on their data rights.

Lack of psychological awareness

According to Moyo and Ndlovu (2022) if a victim steps to report cyberbullying or non-consensual image sharing, they often encounter officers who lack training in digital trauma. The victims often encounter dismissive attitudes, ridicule and lack of privacy which entirely demolishes the public trusting legal remedies. The victims would be asked;

- Victim blaming questions such as "Why did you send the picture?"
- The trauma of the victim repeatedly explaining their experience to different officials.

This lack of psychological awareness within the legal system causes secondary trauma. This causes the victim to feel helplessness as they choose to suffer in silence rather than involve unsupportive legal system.

Regardless, of its reactive shortcomings, Zimbabwe's Cyber and Data Protection Act [Chapter 12:07] has ascertained significant structural and legal milestones since its enactment. The policy fundamentally improved how digital privacy, corporate data processing, and technological crimes are managed nationally. The cabinet's endorsement for the National Child Online Protection Policy (2026-2030) was an outstanding step forward but must be expanded across all sectors.

Strengths

- * Regulatory oversight: Designated the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) as country's official Data Protection Authority.
- * Legal recognition of online harm: The government of Zimbabwe recognized cyber-related offenses through the Cyber and Data Protection Act, making online abuse illegal through establishment of cyber-bullying laws, revenge porn protection and court evidence to convict criminals.
- * Child Protection Focus: The Child Online Protection Framework specifically recognises children as vulnerable population needing protection in digital environments, thus protecting children from harm.
- * Promotion of Cyber security: Government initiatives have increased awareness of responsible internet use and cyber security.
- * Multi-sectoral Approach: The participation of the government, ministries, schools, law enforcement agencies and civil society organizations strengthens policy implementation.

International Practices

The most successful international frameworks for combating cyberbullying combine clear legal definitions, specialized law enforcement, mandatory school programs and platform accountability. Countries that depend solely on criminal penalties often fail, whereas nations using a multi-layered approach including the schools, tech platforms and civil courts accomplish the utmost success rates. Countries such as United States, Australia and United Kingdom have pioneered modern frameworks that force big tech platforms to act quickly. At the US they introduced THE "take it down act" which is an automated screening mechanisms to prevent a deleted intimate image from ever re-upload. Australia is globally recognized on having the "gold standard" best practice for handling non-consensual image sharing and digital abuse, primarily because of its creation of the world's first specialized government regulatory agency, the office of the eSafety Commissioner. Furthermore, it is important to define cyberbullying clearly by its intent to harm, power imbalance and repetitive nature to avoid political abuse. In Zimbabwe, this distinction is legally define under the Cyber and Data Protection Act.

To alleviate the deep psychological trauma caused by cyberbullying, Zimbabwe policy makers must shift from reactive criminal punishments to proactive, psychologically informed structural solutions. Behavioural psychology stresses online behaviour as greatly impulsive, emotionally detached, and accelerated by digital interfaces (Sibanda, 2021). Below, are proposed recommendations to help mitigate cyber bullying;

RECOMMENDATIONS

Treating cyberbullying only after it occurs is an uphill battle. From a community psychology perspective it is imperative to focus on the whole digital ecosystem, preventative systems, collective well-being, and empowering communities to stop digital harms before they occur. That is why, it is fundamental to prevent it, and not just protecting one person but the entire social ecosystem. This approach feels relevant in the digital age, where online communities can either support or harm mental health. Community psychologists therefore, must design

interventions that encourage healthier and more positive online engagement. With that said, we appreciate the government's robust, multi-layered policy framework, to protect its citizens.

Implement sensitization training for law enforcement.

Form specialized "Digital Victim Support units within the (ZRP) so that the officers are able to handle such crimes sensitively, respecting the privacy and the dignity of the victim.

To minimize the talent poaching of ICT experts, they have to be offered structured work options, explicit career progression paths and multi-dimensional financial incentives so that they can help protect the citizens of Zimbabwe. Utilization of AI-driven Security Orchestration, Automation and Response (SOAR) platforms to autonomously manage initial alerts. This inhibits staff burnout and reduces manual workloads.

- **Deploy low Cost, scale-free educational campaigns:** Broad campaigns can be accomplished efficiently by pivoting away from costly traditional media to localized, digital grassroots networks. This can be accomplished by partnering with interactive regional platforms such as CyberZim Challenge to discover and reward digital talent cheaply. Another way is to deploy peer-to-peer training by using present infrastructure to create train-the-trainer cascade effect across rural school hubs.
- **Set-up coordinated fast track reporting mechanisms**
Empowering POTRAZ to host a responsive online grievance portal. This portal should have legal power to release instant take down notices to localized networks and social media platforms to alleviate harm while investigations take place.
- **Collaboration of experts** such as Psychologists and ZRP to work together in establishing more safe channels where victims can safely report abuse online.
- **Educating communities** on consequences of digital harm on cyberbullying to reduce future caseloads on the judicial system.
- **Integrate digital literacy into the National Curriculum**
Studies have shown that criminalization alone may not stop children from abusing each other online, the long term solution must depend on behaviour changes. This can be achieved by online safety modules into primary and secondary curriculum.
- **Create community Tech safety hubs**, Establish hubs where savvy youths can teach older community members and their peers on digital spaces.

CONCLUSION

This paper has displayed that cyberbullying is not just an online drama or an unavoidable part of using technology, but a brutal national crisis that causes major disruptions and drives underreported mental health issues. By instigating the recommendations proposed in this paper, Zimbabwe can shift from reactive system to a proactive protective ecosystem. Digital safety is an essential human right. The internet was designed to connect us not to weaponize against the vulnerable. By taking these necessary steps, Zimbabwe can foster environments defined by human dignity and mutual respect.

REFERENCES

1. Africa Social Work Network (ASWN). (2022). Cyberbullying among high school learners in Zimbabwe: Motives and effects. ASWN Digital Library.
2. Government of Zimbabwe. (2021). Cyber and Data Protection Act [Chapter 12:07]. Zimbabwe Legal Information Institute.
3. Postal and Telecommunications Regulatory Authority of Zimbabwe [POTRAZ]. (2023). Cyber and data protection baseline assessment of Zimbabwean enterprise. POTRAZ Research Reports.potraz.gov.zw
4. Moyo, S., & Ndlovu, N. (2022). Cyberbullying among high school learners in Zimbabwe: Motives, effects, and the institutional vacuum. African Journal of Social Work, 12(4), 185-194. africasocialwork.net

-
5. Chakamba, A. & Zhou, M. (2022). Digital harassment and youth perceptions in Harare Metropolitan Province: Evaluating vulnerabilities in the web era. *International Journal of Research and Innovation in Social Science (IJRISS)*, 6 (4), 621- 628.
 6. Sibanda, M. (2021). Cyberbullying in Higher and Tertiary education institutions in Zimbabwe: Forms, Extent, Effects and Contributing factors. *Journal of Systems Integration* 11 (2):17-27 DOI:10.20470/jsi.v11i2.387
 7. Mawere, D. (2023). Cybersexual harassment in a state University in Zimbabwe: Voices of female students. *The Dyke* 16 (2):1-18 DOI:10.64754/thedyke.v16i2.185