Fighting the Bias:

An Education Guide for Women Leaders, Politicians and Journalists Against Gendered Disinformation

March, **2025**

Acknowledgement

This guide has been developed as a comprehensive resource to equip Ugandan women politicians and journalists with the necessary knowledge and skills to recognise, respond to, and counter disinformation. However, this guide can be used by anyone to recognise, respond and counter gendered disinformation.

The increasing use of digital platforms has brought immense opportunities but also significant challenges, particularly gendered disinformation, which disproportionately affects women in public life.
Women of Uganda Network (WOUGNET), acknowledges the generous financial support of the Association for Progressive Communications, which has enabled the production of this Educational guidebook on Gendered Disinformation.

Disclaimer

This guide was made possible with the generous support of the Association for Progressive Communications (APC). The contents are produced by Women of Uganda Network (WOUGNET) and do not necessarily reflect the views of APC.

List of Abbreviations

AU	African Union
UN	United Nations
UCC	Uganda Communications Commission
CSOs	Civil Society Organizations
2FA	Two-Factor Authentication
VPN	Virtual Private Network
ICT	Information and Communications Technology
NGOs	Non-Governmental Organizations
AI	Artificial Intelligence
E2EE	End-to-End Encryption
APC	Association for Progressive Communications
WOUGNET	Women of Uganda Network
ICFJ	International Center for Journalists
UNESCO	United Nations Educational, Scientific and Cultural Organization
UDHR	The Universal Declaration of Human Rights
CEDAW	The Convention on the Elimination of All Forms of Discrimination Against Women
ODPP	Office of the Director of Public Prosecutions
Wi-Fi	Wireless Fidelity

TABLE OF CONTENTS:

1.0 INTRODUCTION:

1.1 Understanding Gendered Disinformation and Misinformation

Gendered disinformation refers to the deliberate spreading of false or misleading information specifically designed to target individuals based on their gender. It often reinforces stereotypes, discredits women's voices, and deters their participation in public life.[1] It is a subset of broader disinformation campaigns strategically used to undermine women in leadership, journalism, and activism. Unlike general disinformation, gendered disinformation frequently employs sexist narratives, threats of violence, and manipulated media to attack women's credibility and agency.

Gendered misinformation, on the other hand, refers to the unintentional sharing of false or misleading information that perpetuates gender biases. Unlike disinformation, which is spread with the intent to deceive, misinformation is often shared due to a lack of verification or critical digital literacy. Both phenomena contribute to an online environment that is increasingly hostile to women in political and media spaces.

1.2 Gendered Disinformation within the Ugandan Context

In Uganda, gendered disinformation has been on the rise, mainly targeting women politicians, activists, and female journalists. Prominent examples include:

Political Attacks: Women politicians[2] such as Hon. Betty Nambooze, Hon. Zaake Francis' wife Bridget Namirembe, and other female public figures have faced online smear campaigns aimed at discrediting their leadership abilities through gendered narratives portraying them as incompetent, immoral, or unfit for office.

Journalistic Harassment: Female journalists in Uganda frequently experience coordinated online harassment, mainly when covering sensitive political issues. Investigative journalists such as Agather Atuhaire[3] have faced digital attacks intended to silence them and undermine their credibility.

Manipulated Media: Social media platforms in Uganda have been used to spread deepfake images and videos[4]of women leaders and journalists, often in sexually explicit or degrading ways, to damage their reputation and discourage their engagement in public discourse.

1 *OHCHR. (07 August 2023). A/78/288: Gendered disinformation and its implications for the right to freedom of expression – Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression https://www.ohchr.org/en/documents/thematic-reports/a78288-gendered-disinformation-and-its-implications-right-freedom*

2 *Global Voices Advox. (19 January 2025). Gendered disinformation being weaponised against women https://ifex.org/gendered-disinformation-being-weaponised-against-women/*

3 *The Independent. (09 February, 2025). Human rights activist Agather Atuhaire arrested https://www.independent.co.ug/human-rights-activist-agather-atuhaire-arrested/*

4 *Women Press Freedom. (08 December, 2023). distorted Reality: The Alarmingly Growing Use of Deepfakes Against Women Journalists https://www.womeninjournalism.org/opeds/distorted-reality-the-alarmingly-growing-use-of-deepfakes-against-women-journalists*

1.3 Trends and Global Comparisons

Gendered disinformation is not unique to Uganda; it is a growing global trend. Studies by organisations such as the International Center for Journalists (ICFJ)[5] and UNESCO show that female politicians and journalists worldwide face disproportionate online harassment, disinformation campaigns, and cyber threats. Some key trends include:

Coordinated Attacks: Disinformation networks worldwide target women in politics and media to weaken their influence. For instance, research by the Foreign Policy Research Institute highlights how Russian disinformation campaigns[5] have targeted women leaders in Eastern Europe.

Amplification Through Social Media:[7] Platforms like Facebook, Twitter (X), and WhatsApp have become breeding grounds for gendered disinformation due to their algorithmic tendencies to amplify sensational and divisive content.

Intersectionality in Attacks: Women from marginalised communities, including ethnic minorities and LGBTQ+[8] groups, face even harsher forms of disinformation and online abuse.

1.4 Why is this Happening?

The rise of gendered disinformation in Uganda and globally is driven by a combination of deeply rooted societal, political, and technological factors. Patriarchal norms and gender biases continue to fuel narratives that undermine women's leadership and public engagement, reinforcing stereotypes that question their credibility. Politically, disinformation is often weaponised by actors seeking to discredit opponents and maintain existing power structures, disproportionately targeting women in leadership and journalism.[9] Additionally, limited digital literacy among the general population exacerbates the problem, as many unknowingly share false or misleading information without the tools to verify its accuracy. Weak regulatory frameworks, despite the presence of laws such as Uganda's Computer Misuse Act,[10] further enable the unchecked spread of gendered disinformation due to inadequate enforcement mechanisms. Meanwhile, the profit-driven algorithms of social media platforms prioritise engagement over accuracy, amplifying sensational and often harmful gendered narratives. Collectively, these factors create a hostile digital environment that threatens women's participation in public discourse and undermines broader democratic and societal integrity.

5 *ICFJ. (02. 11.2022). The Chilling: A global study of online violence against women journalists https://www.icfj.org/sites/default/files/2023-02/ICFJ%20Unesco_TheChilling_OnlineViolence.pdf*

6 *Foreign Policy Research Institute. (24. January, 2025). The Fight Against Disinformation: A Persistent Challenge for Democracy - Foreign Policy Research Institute https://www.fpri.org/article/2025/01/the-fight-against-disinformation-a-persistent-challenge-for-democracy/*

7 *Sun, Haochen. (2023). Regulating Algorithmic Disinformation https://www.researchgate.net/publication/370751399_Regulating_Algorithmic_Disinformation*

8 *Nile Post. (10 July, 2024). Gender disinformation in the context of LGBTI communities Table of Contents https://nilepost.co.ug/politics/206987/how-gender-focused-misinformation-impacts-women-in-ugandan-politics*

9 *ACT Alliance's Input for the report on gendered disinformation Submitted to the UN Special Rapporteur on Freedom of Expression https://www.ohchr.org/sites/default/files/documents/issues/expression/cfis/gender-justice/subm-a78288-gendered-disinformation-cso-act-alliance.pdf*

10 *Chapter Four. (2022). The Computer Misuse (Amendment) Act, 2022 | Chapter Four https://chapterfouruganda.org/resources/acts-bills/computer-misuse-amendment-act-2022*

1.5 Key Actors in Gendered Disinformation

Understanding the actors[11] involved in gendered disinformation is essential for developing effective counterstrategies, as various groups contribute to its spread differently. State and political actors, including governments and political parties, often weaponise disinformation to silence opposition, with vocal women leaders being prime targets of such campaigns. Troll farms and coordinated networks, driven by political or financial incentives, systematically orchestrate gendered disinformation efforts to manipulate public perception. Traditional and social media also play a significant role, as some outlets amplify sexist narratives or fail to fact-check stories before publishing, further legitimising falsehoods. Additionally, ordinary social media users, whether due to personal biases, misinformation, or a lack of digital literacy, may unknowingly participate in the spread of gendered disinformation. Together, these actors create a complex ecosystem that sustains and reinforces harmful narratives against women, making it imperative to address their roles in counter-disinformation efforts.

1.6 The Need for a Gender-Sensitive Response

Disinformation is a digital threat and a broader societal issue that undermines democracy, freedom of expression, and media integrity.[12] Addressing gendered disinformation requires a multi-faceted approach, including:

- Strengthening digital literacy: Equipping women politicians and female journalists with critical thinking and fact-checking skills.
- Advocating for policy reforms: Enhancing legal frameworks to address online gender-based violence and disinformation.
- Engaging social media Platforms: Holding tech companies accountable for moderating and mitigating gendered disinformation.

11 Nile Post (10 July, 2024). How gender focused misinformation impacts women in Ugandan politics https://nilepost.co.ug/politics/206987/how-gender-focused-misinformation-impacts-women-in-ugandan-politics

12 OECD. (2 February, 2025). Mis- and disinformation https://www.oecd.org/en/topics/sub-issues/disinformation-and-misinformation.html

1.7 Purpose of the Education Guide

This education guide provides a detailed roadmap for women politicians and journalists to recognise, respond to, and counter disinformation through enhanced digital literacy, critical thinking, and online safety measures. The content is tailored to the Ugandan legal and regulatory context, focusing on national, regional, and international frameworks that protect women's rights in digital spaces. By equipping women with the necessary tools and knowledge, this guide empowers them to navigate the digital landscape safely and effectively, ensuring their voices remain strong in public discourse.

2.0. UNDERSTANDING DISINFORMATION

Disinformation refers to false, misleading, or manipulated information deliberately created and spread to deceive an audience. It is often used as a tool for political, ideological, or economic gain. Gendered disinformation specifically targets women and gender minorities, leveraging sexist narratives, harmful stereotypes, and misinformation to undermine their credibility and participation in public life. It manifests in various forms, including false allegations, character assassination, and online harassment, disproportionately affecting women in leadership, media, and activism.

2.1. How Disinformation Affects Women Politicians and Female Journalists

Women politicians and female journalists[13] are particularly vulnerable to disinformation campaigns due to their public visibility and influence. These attacks often aim to discredit their work, erode public trust, and push them out of public spaces. The key impacts include:

Erosion of public trust: Disinformation campaigns systematically undermine the credibility of women leaders and journalists, making it harder for them to influence public discourse. False allegations about corruption, incompetence, or personal scandals are commonly used to discredit them.

Reinforcement of gender stereotypes: Many disinformation narratives exploit traditional gender roles to delegitimise women's contributions. For example, women politicians may be portrayed as emotionally unstable or unqualified for leadership, while female journalists may be depicted as biased or unreliable.

Psychological and emotional impact: Exposure to gendered disinformation can lead to severe mental health issues, including anxiety, depression, and burnout. Many women in the public sphere experience cyberbullying, threats, and derogatory remarks, leading to self-censorship and withdrawal from public platforms.

Threat to safety and security: Disinformation campaigns can escalate into real-world threats, including physical violence, stalking, and harassment. Women facing targeted attacks often receive threats against themselves and their families, creating a climate of fear.

Suppression of political and media participation: Many women reconsider or abandon careers in politics or journalism due to the hostile online environment created by disinformation campaigns. This limits diversity in leadership and media, reinforcing systemic gender inequalities.

13 *Nile Post. (10. 07. 2024). How gender focused misinformation impacts women in Ugandan politics https://nilepost.co.ug/politics/206987/how-gender-focused-misinformation-impacts-women-in-ugandan-politics*

2.2. Common Forms of Gendered Disinformation

Gendered disinformation takes multiple forms, leveraging digital tools and social media to spread false narratives. Common tactics include:

Manipulated images and videos (Deepfakes): Deepfake technology is increasingly used to create misleading visuals, such as doctored videos that depict women in compromising or inappropriate situations. These manipulated images can damage reputations and spread falsehoods rapidly.

Fabricated news stories: False news articles and social media posts are created to misrepresent women's actions, policies, or personal lives. These stories often go viral, influencing public opinion before they can be debunked.

Online harassment campaigns: Coordinated efforts by troll networks and bot accounts aim to intimidate and silence women through cyberbullying, hate speech, and mass reporting of their social media profiles.

Doxxing: The malicious act of exposing personal information, such as home addresses, phone numbers, and private emails, to threaten and endanger women's safety. This tactic is used to intimidate and drive women out of public discourse.

Gendered memes and hashtags: Disinformation campaigns frequently use misogynistic memes and trending hashtags to spread false narratives and ridicule women in politics and media. These online trends reinforce harmful stereotypes and diminish their credibility.

3.0 ADDRESSING GENDERED DISINFORMATION: LEGAL FRAMEWORKS, REPORTING MECHANISMS, AND POLICY CONCERNS

Uganda has several laws and regulations addressing online safety, cybercrime, and digital rights. While not all are explicitly gender-focused, they offer avenues for tackling gendered disinformation, online harassment, and digital safety concerns. Below are the key laws and their applications.

3.1 The Computer Misuse Act, 2011 (As amended)

The Computer Misuse Act (2011) was amended in 2022[14] to strengthen laws against cyber harassment and misuse of online platforms.

Key Provisions:

- Section 12: Criminalizes sending malicious, misleading, or false information online.
- Section 24: Defines and penalizes cyber harassment, including targeted abuse against women.
- Section 26: Addresses unauthorised access to data, protecting against doxxing and hacking that can target women and activists.
- Section 26D (1): Criminalizes the misuse of social media.

Concerns:

- While it criminalises online abuse and misinformation, it has been criticised for potentially stifling freedom of expression, with vague definitions that can be misused against activists, journalists, and women's rights defenders.

3.2 The Data Protection and Privacy Act, 2019[15]

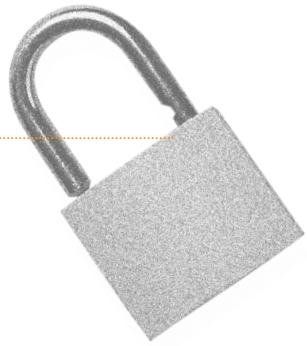
This law governs the collection, processing, and protection of personal data. It is essential in combating online privacy violations such as doxxing, cyberstalking, and gender-based digital abuse.

Key Provisions:

- Right to Privacy: Ensures individuals' personal data is protected from unauthorized access.
- Consent Requirement: Organisations must obtain consent before collecting and sharing personal data.
- Protection Against Doxxing: Makes it illegal to publicly share personal information without consent, which is often used to target women and activists online.
- Penalties for Violations: Those found guilty of data breaches face fines or imprisonment.

Concerns:

- Enforcement remains weak, and many victims of digital privacy violations struggle to get justice due to lack of awareness and reporting mechanisms.



14 Chapter Four. (2022). The Computer Misuse (Amendment) Act, 2022 | https://chapterfouruganda.org/resources/acts-bills/computer-misuse-amendment-act-2022

15 Grant Thornton. (2019). Data Protection and Privacy Act of Uganda, 2019 https://www.gtuganda.co.ug/globalassets/1.-member-firms/uganda/media/pdf-documents/data-protection-and-privacy-act-of-uganda.pdf

3.3 The Penal Code Act (Cap 128)[16]

Although initially designed for offline crimes, the Penal Code Act has sections that can be applied to online defamation, harassment, and hate speech.

Relevant Provisions:

- Section 179: This covers defamation, including false and harmful statements spread online.
- Section 180: Criminalizes publishing false information that harms a person's reputation.
- Section 181: Penalizes incitement to violence, which can apply to online gender-based threats.

Concerns:

- The burden of proof is high, making it difficult for women facing online abuse to secure convictions.

3.4 The Uganda Communications Act, 2013[17]

This Act regulates electronic communication and media content in Uganda. It gives powers to the Uganda Communications Commission (UCC) to monitor, regulate, and enforce laws on digital platforms.

Key Provisions:

- Section 5: Gives UCC authority to regulate online communication platforms.
- Section 31: Requires all telecommunication and digital service providers to comply with minimum broadcasting standards.
- Section 41 allows for suspending or blocking harmful online content, including hate speech and gendered disinformation.

Concerns:

- Some provisions have been used to suppress online activism, raising concerns about censorship and over-regulation.

16 *FIA. (2025). The penal code act chapter 120. https://www.fia.go.ug/sites/default/files/downloads/Penal%20Code%20Act.pdf*

17 *UCC. (2025). Uganda Communications Act, 2013 https://www.ucc.co.ug/download/uganda-communications-act-2013/*

3.5 The Prevention of Trafficking in Persons Act, 2009[18]

While focused on human trafficking, this law also protects victims of online sexual exploitation and cyber-trafficking, particularly women and girls.

Relevant Sections:

- Criminalises online recruitment and grooming for sexual exploitation.
- Prohibits the creation and distribution of exploitative digital content involving victims.

Concerns:

A key concern is that the Prevention of Trafficking in Persons Act, 2009 does not comprehensively address the evolving tactics of cyber-trafficking, leaving gaps in enforcement and victim protection, especially in cases involving complex digital platforms and cross-border crimes.

3.6 The Domestic Violence Act, 2010

This Act primarily addresses offline domestic violence but can apply to cyber harassment within intimate relationships.

Key Provisions:

- Protects victims of emotional and psychological abuse, which includes online stalking, threats, and harassment.
- Allows for protective orders against perpetrators, including those using digital means to harass partners or ex-partners.

Concerns:

A key concern is that the Domestic Violence Act, 2010, primarily focuses on offline abuse and lacks explicit provisions addressing the complexities of cyber harassment. This may limit its effectiveness in protecting victims from emerging forms of digital abuse within intimate relationships.

18 *ULII. (23. 10. 2009). Prevention of Trafficking in Persons Act, 2009 - ULII https://ulii.org/akn/ug/act/2009/7/eng@2009-10-23*

3.7. Regional and International Legal Instruments

Uganda is a signatory to multiple regional and international treaties that address gender equality, freedom of expression, and digital rights:

African Charter on Human and Peoples' Rights:[19] Protects freedom of expression and information, emphasizing the need for fair media representation.

The Maputo Protocol (2003):[20] Advocates for women's rights, including their protection from gender-based violence and participation in governance.

The Universal Declaration of Human Rights (UDHR, 1948): Guarantees freedom of speech and media rights and forms a foundational international standard.

The Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW, 1979): Calls for gender equality in political and media spaces, addressing barriers posed by disinformation and online abuse.[21]

19 *African Union (2025). African Charter on Human and Peoples' Rights https://au.int/en/treaties/african-charter-human-and-peoples-rights*

20 *Equality Now. (2025). The Maputo Protocol: Protecting African Women's Rights - Equality Now https://equalitynow.org/promoting_african_womens_rights/*

21 *OHCHR . (18 December, 1979) Convention on the Elimination of All Forms of Discrimination against Women New York https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-elimination-all-forms-discrimination-against-women*

3.8. Reporting Mechanisms for Gendered Disinformation

Victims of gendered disinformation in Uganda can seek legal and institutional support through the following mechanisms:

- Uganda Police Force, Cybercrime Unit:[22] Handles cases of online harassment, cyberbullying, and digital threats.
- Uganda Communications Commission (UCC)[23] Regulates online content and provides a channel for reporting harmful digital campaigns.
- Directorate of Public Prosecutions (DPP):[24] Investigates and prosecutes cyber-related crimes, including gendered disinformation.
- Personal Data Protection Office (PDPO): Monitors, investigates and reports on the observance of the right to privacy and of personal data.
- Civil Society Organizations (CSOs): Women's Rights Organizations and Digital Human Rights organizations offer legal support, advocacy, and digital security training.
- Social Media Reporting Tools: Platforms like Facebook, Twitter (X), and Instagram have reporting features for abusive content and disinformation.

Addressing gendered disinformation requires a multi-stakeholder approach, combining legal action, digital literacy, and advocacy to create safer online space.

22 *African Union (2025). African Charter on Human and Peoples' Rights https://au.int/en/treaties/african-charter-human-and-peoples-rights*
23 *Equality Now. (2025). The Maputo Protocol: Protecting African Women's Rights - Equality Now https://equalitynow.org/promoting_african_womens_rights/*
24 *OHCHR . (18 December, 1979) Convention on the Elimination of All Forms of Discrimination against Women New York https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-elimination-all-forms-discrimination-against-women*

4.0 DIGITAL LITERACY AND CRITICAL THINKING

Recognizing Disinformation Online

Gendered disinformation is a form of online abuse that disproportionately targets women and marginalized groups, often aiming to silence their voices, damage reputations, or discourage political participation. Strengthening digital literacy and critical thinking is essential in identifying and countering false information online.

Below are key strategies for recognizing disinformation:

- **dentifying Misleading Headlines:** Disinformation often spreads through sensationalist or misleading headlines designed to provoke emotional reactions. Critical readers should analyse headlines carefully, looking for exaggerations, loaded language, or inconsistencies with the article's content.

- **Cross-Checking Sources for Credibility:** Reliable news sources follow journalistic standards and cite verifiable evidence. Before believing or sharing information, it is essential to cross-check multiple credible sources, such as reputable news agencies, government websites, and recognised fact-checking organizations.

- **Using Fact-Checking Tools and Platforms:** Various platforms specialize in verifying the accuracy of online content. Some key fact-checking platforms include:

    - **Africa Check** – An independent African fact-checking organisation.
    - **PesaCheck** – A fact-checking initiative focused on misinformation in East Africa.
    - **Google Fact Check Tools** – Helps verify claims from various sources worldwide.

By employing these techniques, individuals can critically assess online content, reducing the spread of falsehoods that often target women leaders, activists, and professionals.

Countering Disinformation

Identifying false content is just the first step; taking action to counter disinformation ensures a more truthful and inclusive online space. Effective strategies include:

- Reporting False Content on Social Media: Most social media platforms provide mechanisms to report false or harmful content. Reporting misleading or abusive posts helps prevent their spread and holds perpetrators accountable.
- Engaging with Credible Media Organizations: Supporting and promoting trusted journalism counters false narratives. Engaging with responsible media outlets by sharing accurate articles and amplifying credible voices strengthens fact-based discourse.
- Developing Counter-Narratives to Challenge Falsehoods: Counter-narratives involve creating and sharing accurate, compelling content that debunks misinformation. This includes writing blogs, producing videos, or engaging in discussions that correct false claims, particularly those targeting women and vulnerable groups.

5.0: ONLINE SAFETY AND DIGITAL SECURITY

Online safety and digital security practices are critical in countering gendered disinformation and ensuring that women, activists, and marginalised groups can participate safely in digital spaces. Disinformation campaigns often target women with false narratives, harassment, and privacy breaches, aiming to silence their voices and undermine their credibility. Strengthening online safety measures protects individuals from cyber threats such as doxxing, identity theft, and online abuse. By adopting robust digital security practices, women can safeguard their personal information, prevent cyberattacks, and maintain their ability to engage freely in online discussions without fear of harassment or retaliation.

5.1 Protecting Personal Data

Women and activists targeted by gendered disinformation often face threats such as doxxing (publishing personal information without consent) and identity theft. To safeguard personal information, individuals should:

- Use Strong Passwords and Two-Factor Authentication:
  - Create complex, unique passwords for each online account using letters, numbers, and characters such as Th3C4tA1w4y5L4ands0nF33t!.
  - Use a password manager to store credentials securely such as Bitwarden, LastPass.
  - Enable two-factor authentication (2FA) on all accounts to add an extra layer of security.
  - Regularly update passwords and avoid reusing them across multiple platforms.

- Avoid Oversharing Personal Information Online:
  - Limit the sharing of sensitive information, such as home addresses, phone numbers, and location details on social media.
  - Adjust privacy settings on social media platforms to restrict access to personal data.
  - Be cautious when filling out online forms or surveys that request personal details.
  - Use pseudonyms or alternative email addresses when signing up for non-essential online services.
  - Regularly review and clean up old posts or accounts that may reveal personal information.

- Secure Social Media and Email Accounts:
  - Enable security notifications to detect suspicious login attempts.
  - Avoid logging into personal accounts on public or shared devices.
  - Revoke unnecessary third-party app permissions that may have access to personal data.

5.2 Additional Online Safety and Digital Security Measures

To further enhance online security, individuals should adopt the following practices:

- Use Secure Internet Connections:
  - Avoid using public Wi-Fi for sensitive transactions unless connected to a Virtual Private Network (VPN).
  - Ensure home Wi-Fi is protected with a strong password and encrypted settings.
  - Disconnect devices from Wi-Fi when not in use to prevent unauthorised access.

- Protect Devices from Cyber Threats:
  - Keep software, operating systems, and applications updated to patch security vulnerabilities.
  - Install reputable antivirus and anti-malware programs to detect and remove threats.
  - Enable device encryption to protect stored data in case of theft or loss.

- Be Cautious of Phishing and Scams:

Phishing: Phishing is a cyber-attack where scammers trick people into revealing sensitive information like passwords or credit card numbers, usually through fake emails, links or websites.

Scams: Scams are fraudulent schemes designed to deceive people and steal their money, personal information, or assets by gaining their trust or exploiting their lack of awareness.

  - Verify email senders before clicking on links or downloading attachments.
  - Do not share login credentials or personal information with unverified contacts.
  - Report phishing attempts to platform security teams or cybersecurity agencies.

- Enable Account Recovery Options:
  - Set up backup recovery methods such as security questions or alternative email addresses.
  - Regularly review and update account recovery settings to prevent unauthorized access.

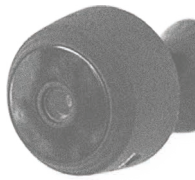
5.3 Dealing with Online Harassment

Gendered disinformation often accompanies cyber harassment, including trolling, threats, and non-consensual image distribution or circulation. Effective strategies to handle online harassment include:

- Blocking and Reporting Abusive Accounts: Most social media platforms allow users to block harassers and report abusive content. Consistently reporting violations increases platform accountability in enforcing community standards.

- Seeking Legal Action Against Cyber Harassment: In Uganda, laws such as the Computer Misuse Act, 2022, and the Anti-Pornography Act of 2014, provide legal avenues for victims of cyber harassment. Individuals experiencing severe online abuse should:
  - Document evidence, including screenshots, URLs, and timestamps of abusive messages.
  - Report incidents to the Uganda Communications Commission (UCC) and local law enforcement authorities.
  - Consult legal experts or digital rights organizations for assistance in taking legal action.

- Accessing Psychological Support and Peer Networks: Online harassment can cause emotional distress and mental health challenges. Victims should seek:
  - Counseling or psychological support services.
  - Online and offline peer networks that provide emotional support and advocacy.
  - Digital self-care strategies to manage online stress and maintain mental well-being.



5.4 Safe Online Communication

Maintaining secure and private communication channels is crucial in preventing data leaks, cyberstalking, and surveillance. Recommended practices include:

- Using Encrypted Messaging Services: Platforms like Signal, Telegram (Secret Chats), and WhatsApp (end-to-end encryption) offer more secure communication than regular text messaging or emails.

- Verifying Sources Before Sharing Information: Before forwarding messages, individuals should:
  - Confirm the authenticity of the source.
  - Cross-check with official sources or fact-checking organizations.
  - Avoid amplifying unverified claims that may contribute to misinformation.

- Practicing Safe Online Behavior:
  - Think critically before sharing sensitive opinions or personal experiences in public forums.
  - Be cautious when engaging with unknown contacts, especially those requesting personal information.
  - Join trusted and moderated online communities that prioritize digital safety.

Through effective online safety and digital security practices, individuals can navigate online spaces more safely and confidently, reducing the risks associated with gendered disinformation and cyber threats. Digital literacy and online safety are essential tools in combating gendered disinformation and ensuring a secure digital environment for all. By recognizing and countering disinformation, protecting personal data, dealing with online harassment, and practicing safe online communication, individuals can create a more inclusive and respectful online space. Strengthening these capacities not only empowers women and marginalized groups but also contributes to a more accountable and fact-based digital landscape.

6.0 RECOMMENDATIONS TO COUNTER GENDERED DISINFORMATION

Combating gendered disinformation requires a multi-faceted approach that includes strengthening digital literacy, improving legal protections, holding social media platforms accountable, promoting women's digital leadership, and fostering multi-stakeholder collaborations. By implementing these recommendations, governments, organizations, and individuals can create a safer, more inclusive, and equitable digital space for all.

6.1 Strengthening Digital Literacy and Awareness

Incorporate digital literacy in education systems: Governments and educational institutions should integrate digital literacy, critical thinking, and media analysis into school curricula to equip young people with skills to identify and counter disinformation.

Conduct community-based digital literacy programs: Civil society organizations (CSOs) and digital rights groups should organize workshops and campaigns to educate women, activists, and the general public on identifying and responding to gendered disinformation.

Encourage responsible digital engagement: Social media users should be trained to critically assess information before sharing, ensuring they do not amplify harmful narratives targeting women.

6.2 Strengthening Legal and Policy Frameworks

Enhance legal protections against online harassment and disinformation: Governments should review and strengthen existing laws to ensure they adequately protect individuals, particularly women, from digital threats and gendered disinformation.

Ensure effective law enforcement implementation: Law enforcement agencies must be trained and equipped to handle cyber crimes related to gendered disinformation, online harassment, and digital violence.

Develop platform-specific regulations: Governments and regulatory bodies should work with social media companies to implement policies that effectively detect, remove, and prevent the spread of gendered disinformation.

6.3 Strengthening Social Media Accountability

Improve content moderation policies: Social media platforms should develop more robust content moderation practices to quickly identify and address gendered disinformation.
Increase transparency in reporting mechanisms: Platforms should provide clearer and more efficient channels for reporting abusive content, ensuring that victims of gendered disinformation receive timely support and resolution.

Promote ethical AI use in content moderation: Technology companies should develop and utilise artificial intelligence tools to detect and prevent gender-based online abuse while ensuring they do not disproportionately silence women's voices.

6.4 Promoting Women's Digital Leadership and Representation

Support women in digital advocacy and journalism: Governments, private sector players, and civil society should invest in programs that empower women to take leadership roles in digital spaces, including technology, journalism, and advocacy.

Create safe online spaces for women: Platforms and communities should establish digital forums and support networks that offer protection and mentorship to women engaging online.

Amplify women's voices in media: Media outlets should actively feature women's perspectives and stories, countering harmful narratives with positive and factual representations.

6.5 Enhancing Collaboration and Multi-Stakeholder Engagement

Encourage cross-sector partnerships: Governments, CSOs, academia, and private tech companies should collaborate to design comprehensive solutions to tackle gendered disinformation.

Support regional and international efforts: Engagement with African Union (AU), United Nations (UN), and other international bodies can strengthen coordinated responses to gendered digital threats.

Encourage grassroots movements and advocacy: Supporting local advocacy efforts ensures that responses to gendered disinformation are inclusive and contextually relevant.

6.6 Providing Mental and Psychological Support for Survivors of Gendered Disinformation

To counter gendered disinformation, it is crucial to provide mental and psychological support for victims and survivors. Establishing safe spaces both online and offline where they can access counseling, peer support, and trauma-informed care helps mitigate the emotional toll of digital attacks. Integrating digital resilience and training with mental health resources empowers affected individuals to rebuild confidence and safely re-engage in online spaces. Additionally, collaboration with psychologists, gender experts, and digital rights organizations can ensure a holistic approach to healing and empowerment.

Within the Ugandan context, victims and survivors of gendered disinformation can access mental and psychological support through various organizations and institutions. Civil society organizations such as Mental Health Uganda[25] and StrongMinds[26] provide mental health counseling tailored to trauma and online abuse. However, more needs to be done to strengthen tailored counselling for gendered disinformation. Government health facilities and community-based initiatives also offer psychological support services, while legal aid organizations such as FIDA [27] and Women's Probono Initiative[28] can assist with justice and redress mechanisms.

25 *Mental Health Uganda (2025) https://www.mentalhealthuganda.org/*
26 *StrongMinds. (2025) https://strongminds.org/*
27 *FIDA – UGANDA (2025). https://strongminds.org/*
28 *Women's Probono Initiative (2025) https://womenprobono.org/*

7.0 CONCLUSION

In an increasingly digital world, gendered disinformation poses a significant threat to women's rights, freedom of expression, and democratic participation. This legal guidebook has explored the legal frameworks, digital literacy strategies, and online safety measures necessary to counteract the spread of gendered disinformation. It has also provided key recommendations to empower individuals, organisations, and policymakers in tackling this pervasive issue.

Strengthening legal protections, enhancing digital literacy, and promoting responsible technology use are essential steps in mitigating the harmful effects of gendered disinformation. By fostering collaboration between governments, civil society organisations, media, and technology companies, we can create a more inclusive and equitable online environment where women can safely express themselves and participate in digital spaces without fear of harassment or targeted attacks.

The fight against gendered disinformation requires sustained efforts, proactive policies, and a collective commitment to digital rights and online safety.

References

- African Union. (2003). Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa (Maputo Protocol). African Union. Retrieved from *https://au.int/en/treaties*
- Association for Progressive Communications. (n.d.). Gendered disinformation and online gender-based violence: Emerging threats to democracy, digital rights, and gender justice. Retrieved from *https://www.apc.org*
- Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW). (1979). United Nations. Retrieved from *https://www.un.org/womenwatch/daw/cedaw/*
- International Center for Journalists. (2020). Troll armies, disinformation, and gendered attacks: The state of online violence against women journalists. Retrieved from *https://www.icfj.org*
- PesaCheck. (n.d.). Fact-checking gendered disinformation in East Africa. Retrieved from *https://pesacheck.org*
- Uganda Communications Act, 2013. (2013). Government of Uganda.
- Uganda Communications Commission. (n.d.). Regulations on digital safety and content moderation. Retrieved from *https://www.ucc.co.ug*
- Uganda Penal Code Act (Cap 120). (1950). Government of Uganda, Chapter 128 *https://ulii.org/akn/ug/act/ord/1950/12/eng@2014-05-09*
- Uganda Computer Misuse (Amendment) Act, 2022. (2022). Government of Uganda. *https://chapterfouruganda.org/sites/default/files/downloads/The-Computer-Misuse-%28Amendment%29-Act-2022.pdf*
- Uganda Data Protection and Privacy Act, 2019. (2019). Government of Uganda. *https://media.ulii.org/media/legislation/18002/source_file/d9cc089540b7bca1/2019-9.pdf*
- United Nations Educational, Scientific and Cultural Organization (UNESCO). (2021). The Chilling: Global trends in online violence against women journalists. Retrieved from *https://en.unesco.org*
- United Nations General Assembly. (1948). The Universal Declaration of Human Rights. Retrieved from *https://www.un.org/en/about-us/universal-declaration-of-human-rights*
- Wilson Center. (2020). Gendered disinformation and the global information ecosystem. Retrieved from *https://www.wilsoncenter.org*

About WOUGNET

Women of Uganda Network (WOUGNET) is a non-governmental organization initiated in May 2000 by several women's organizations in Uganda to develop the use of information and communication technologies (ICTs) among women as tools to share information and address issues collectively. The organization envisions an inclusive and just society where women and girls are enabled to use Information Communications Technologies (ICTs) for sustainable development.

We thank the Association for Progressive Communications (APC) for the generous financial support that made the publication of this education guide possible.

Women of Uganda Network
Plot 67 Namuwongo, Bukasa Road
P.O Box 138387, Kampala, Uganda Tel: +256 394 823109
Email: info@wougnet.org

www.wougnet.org

Women of Uganda Network *@wougnet* *@wougnet1*