How to Identify and Counter Online Gendered Disinformation A Handbook

How to Identify and Counter Online Gendered Disinformation

A Handbook

PANOS
SOUTH ASIA

Compiled by **Smita Magar**
Edited by **Sewa Bhattarai**, **Shabdakarmi Ventures**
Illustrations by **Prashna Budha Magar**

PANOS SOUTH ASIA
391/55, Samudaik Bhawan Marg
Lalitpur, Kathmandu, 44700 Nepal
Website: www.panossouthasia.org

GLOSSARY

Algorithm Bias: Social media companies profit from engaging people on their platforms, which is easiest for them to do by 'recommending' things similar to what you have liked or most engaged with. So, algorithms can curate content according to your online activities and to maximize engagement, often creating a bubble of similar information flow including stereotypical biases. This strengthens and reinforces your biases and prejudices further.

Fact Check: A set of practices and tools used to verify information. It is conducted before or after the content is published or disseminated.

Gendered Disinformation: Information that targets women or gender diverse people, and draws its content from sexism, misogyny, and stereotypical gender roles.

Information Disorder: Creation and distribution of inaccurate information. The content could be based on propaganda, lies, rumours, hoaxes, hyper-partisan content, falsehoods or manipulated media. Misinformation, disinformation, and malinformation are collectively understood as information disorder.

Malign Actors: Disinformation expert Nina Jankowicz defines the term as 'malign individuals or organisations on the internet who are using disinformation to achieve political effect or influence the conversation'.

Online: Any communication that uses the internet, including email, social media platforms (such as Facebook, Twitter, Instagram, TikTok, YouTube), messaging apps (such as Facebook Messenger, WhatsApp, Signal, Viber), blogging platforms (such as WordPress, Medium), video conference platforms (Zoom, Google Meet, Jitsi), websites, etc.

Online Violence: Any form of violence that is expressed in the virtual world through use of internet and technology. It includes threats of physical harm, abusive texts, images and videos, harassment, defamation, sexual abuse, discrimination based on gender, race, class or caste, doxing, and so on. Online violence has offline consequences.

Online Gender-Based Violence: Online gender-based violence occurs when women and gender diverse people face violence in online spaces because of their gender.

De-platform: To prevent an individual or a group from participating in a social media platform, forum, or debate. This is usually done by blocking the accounts of those who hold views regarded as unacceptable or offensive, removing their accounts, or targeting them with overwhelming abuse. It can be done by individuals, groups, tech companies, or institutions.

Trigger Warning: This handbook contains description of types and examples of online gender-based violence.

TABLE OF CONTENTS

INTRODUCTION

The advent of internet and technology has allowed us to access any information we need with a click or a swipe. However, in this hyper-connected world, exponentially pervasive creation and dissemination of unreliable, inaccurate, and deceptive information that cause harm is resulting in information disorder.[1] This creates a hostile environment that manipulates opinions and silences voices of reason with long-term consequences.

> *Example: Even though politician Hisila Yami won the case against the magazine 'Crime Today' that published a false story claiming that she was 'the most corrupt woman in South Asia', the negative impact of it in general psyche still lingers.*[2]

There are mainly three types of inaccurate and deceptive information that are contributing to information disorder.

- **Misinformation** is false information that is unknowingly created or shared, without the intention to mislead.

  Example: Online news portal 'Setopati' published a news report titled 'These are the 55 mayoral and 37 deputy mayoral candidates of Kathmandu Metropolitan city'. NepalFactCheck.org fact checked and found that there were only 30 deputy mayoral candidates.[3]

- **Disinformation** is false information or content that is deliberately created and knowingly shared to deceive or cause harm. It can be targeted to a particular race, gender, ethnicity or marginalised group.

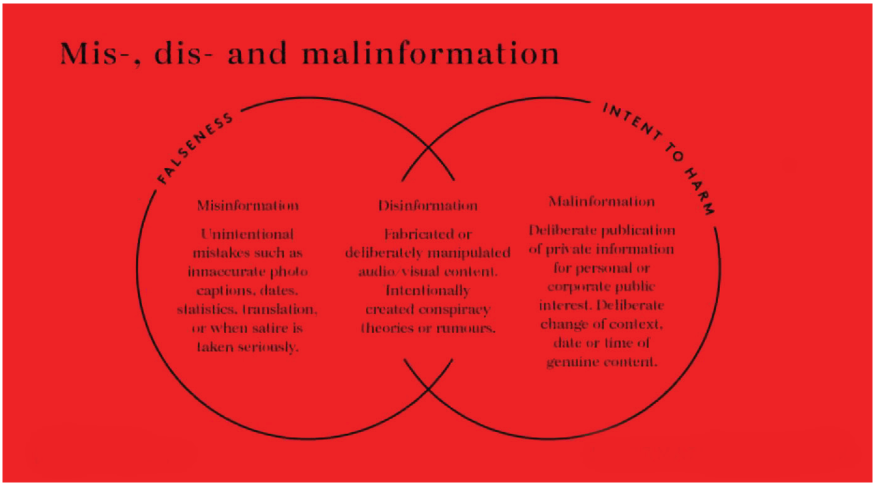
  Example: On 3rd May 2022, multiple online news websites published news reports claiming that a complaint has been filed at the Commission for the Investigation of Abuse of Authority against Sunita Dangol, a CPN-UML deputy mayoral candidate in Kathmandu Metropolitan City. The complaints allegedly claimed that she had falsified her educational certificate and had engaged in corruption at her job. It was fact-checked and found to be not true.[4]

[1] Wardle, C. (2019)
[2] Yami (2021)
[3] NepalFactCheck.org (2022a)
[4] NepalFactCheck.org (2022b)

- **Malinformation** is the distribution of mostly truthful information with intent to harm. It is an intentional act of often sharing private information of someone in public through texts, images, and videos.

  Example: On 9th October 2002, 'Jana Aastha' *published an article titled 'A colourful evening in Film city' with actress Shrisha Karki's nude picture. Karki died by suicide after six days.*[5]

Information disorder is not a new phenomenon, but internet and social media have made it much more pervasive. Online, it crosses borders and socio-cultural-economic barriers, is undisrupted by time and space, and gets a sense of anonymity. While it affects everyone, it disproportionately impacts women and marginalised groups with much more severe consequences.



Mis-, dis- and malinformation

Misinformation

Unintentional mistakes such as innaccurate photo captions, dates, statistics, translation, or when satire is taken seriously.

Disinformation

Fabricated or deliberately manipulated audio/visual content. Intentionally created conspiracy theories or rumours.

Malinformation

Deliberate publication of private information for personal or corporate public interest. Deliberate change of context, date or time of genuine content.

Image Source: First Draft's Essential Guide to Understanding Information Disorder, 2019

Gendered Disinformation is a Threat to Democracy

Politically motivated online gendered disinformation campaigns are one of the most serious hurdles to women's full and equal political participation. They are designed to discourage and restrict the political participation of women by creating hostile online environments for them. The aim of these acts of online violence directed towards women politicians, voters, civil and political activists is to achieve one or all the following results:

[5] Thapa, M. (2002)

Silencing and De-platforming	To silence them, push them out of the political discourse and de-platform them from social media.
Sending a Chilling Message	Send a ‘chilling message’ to all women that it is ‘unsafe’ to participate in elections, have and share views on civil and political rights, and aspire for political career or public office.[6]
Forcing them to withdraw	Make women, gender diverse people, and marginalised communities withdraw from voting, activism, and leadership by creating hostile environment through co-ordinated harassment and cyber-attacks.
Alter Public Opinion	To manipulate public understanding of female politicians in order to make them appear unfit, unlikeable, unworthy, untrustworthy, and unqualified for politics.

Hence, gendered disinformation adversely impacts women’s full and equal participation in politics, influences elections, and weakens women’s rights, resulting in a threat to democracy and fair elections. Therefore, as members of civil society, it is our duty to monitor social media and identify and tackle gendered disinformation to create a healthy and safe digital environment for women, gender diverse people and minorities.

Why a Handbook?

Various researches show that information disorder increases exponentially during election campaigns. Nepal is not an exception to this. In recent times, social media has become a notorious platform for spreading of information disorder. During elections, candidates of all genders are targeted. However, because of existing socio-cultural and structural biases, the nature and motive of attacks and negative impact upon women, gender diverse people, and marginalised communities are different. These attacks during elections are often made by malign actors and politically motivated trolls and bots that aim to manipulate political or electoral outcomes. So, gendered disinformation not only affects the career and wellbeing of women politicians negatively; but also destroys public confidence in them and negatively influences the ability

[6] NDI (2021c)

of citizens to make informed political choices. In the long term, this threatens democracy and fair elections, and discourages women's participation in public spaces.

In this context, 'A Handbook to Identify and Counter Online Gendered Disinformation' has been prepared as part of a series on social media monitoring. It aims to create awareness about online gender-based violence and gendered disinformation. It aims to support users in recognising and countering these forms of online violence.

Panos is also releasing a subsequent handbook focused on the more technical aspects of collecting and analysing social media data to detect early warning signs and trends related to gendered disinformation and online violence against women in politics. Both handbooks are available at https://www.panosa.org/resources/

Who is It for?

This handbook is prepared for social media users – from the public to politicians, journalists, human rights defenders, activists, and civil society members. It aims to provide users with a handy guide to identifying and countering online gendered disinformation while being safe in the virtual world. Its objective is not only to support users in being digitally safe, but also to help users avoid unintentionally committing online violence against women and gender diverse people.

UNDERSTANDING GENDERED DISINFORMATION

Gendered disinformation can be understood as "the spread of deceptive or inaccurate information and images against women political leaders, journalists, and female public figures, following story lines that often draw on misogyny, as well as gender stereotypes around the role of women. This type of disinformation is designed to alter public understanding of female politicians' track records for immediate political gain, as well as discourage women seeking political careers."[7]

> *Example: On 20th December 2021, a weekly 'Ghatana ra Bichar' published a news headlined 'The secret to Padma's progress' which mentions that the former minister Padma Aryal won the position of Party Secretary in the 10th general convention of CPN-UML party due to her connection with the party's powerful leader Bishnu Paudel, who is her father-in-law.*[8]

This article undermines the former minister Aryal's capability as a politician. It tries to create a public opinion of her political career as being dependent on a close male relative, while dismissing her political achievements. Such gendered disinformation is intentionally created to cause harm.

1. How is it different from other gender-based violence (GBV)?

Gendered disinformation is a combination of misogyny, sexism, disinformation, and online violence. It is slightly different from other forms of gender-based violence in that it generally targets women and gender diverse

[7] Heinrich-Boll-Stiftung European Union (2021)

[8] PSA (2022)

people who are in high positions of power or occupy public spaces. It can be very targeted and can have a visual element to it. It also has a degree of co-ordination and ‘malign intent’ of silencing, embarrassing or disparaging the target in some way.[9]

GENDERED DISINFORMATION

Target	▪ Women and gender diverse people who are in positions of power, occupy public spaces, or advocate for gender and minority rights. ▪ Example: women politicians, journalists, activists, human rights defenders, LGBTIQA+ and marginalised communities.
Perpetrators	▪ Malign actors: Individuals or groups that are authoritative, illiberal, undemocratic, and supporters of patriarchy. ▪ Lone or coordinated actors who may be ideologues, members of extremist or fringe groups, or pursuing financial gain.
Motive	▪ To shame, humiliate, embarrass, and disparage women. ▪ To silence and de-platform them from social media. ▪ To demean and scare women and their families. ▪ To convince the public that women are not fit for public positions and spaces. ▪ To insist that women politician are unqualified, untrustworthy, unworthy, and unlikeable. ▪ To discourage other women from using online platforms, expressing their opinions or seeking public positions of power. ▪ During political campaigns, it is designed not only to scare women and gender diverse people from participating in the elections as candidates and voters, but also to alter public opinions and election outcomes.

Note: The methods and tactics of disinformation are described in detail in a separate table on page 9.

2. Categories of Gendered Disinformation

Panos South Asia (PSA) has identified five categories of gendered disinformation and online violence against women politicians that we should watch out for in order to counter them effectively.

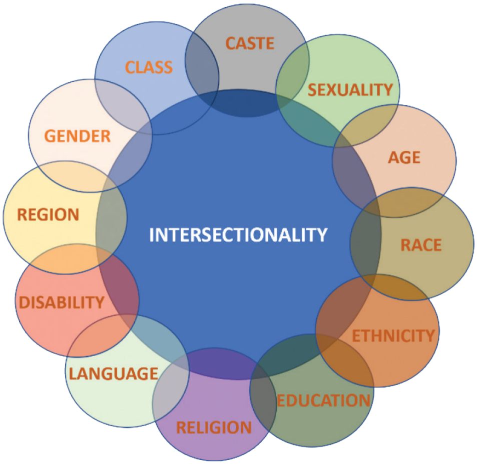
[9] NDI (2021a)

CATEGORY	DEFINITION	EXAMPLES
Insult and hate speech	Comments involving insults and hate.	*Bitch, prostitute, widow, slut.*
Embarrassment/ reputational risk	Serious negative remarks about a woman's character, mostly through attacks on morality and sexuality.	*"You slept with so and so", "You are someone's mistress."*
Physical threats	Remarks threatening a woman with physical violence.	*"I will beat you up", "I will rape you."*
Sexualised distortion	Use of texts, images or videos with sexualised distortion and insulting remarks containing stereotypes about women's traditional roles.	*"You should get married and bear children", "Your place is in the kitchen", "Women should be seen, not heard."*
Undermining of ability	Remarks that undermine women's abilities as leaders or attribute/link their success to their more powerful friends or relatives.	*"You were appointed because of your father's political influence", "You landed the job because of the CEO is your uncle's friend."*

Source: PSA (2022)

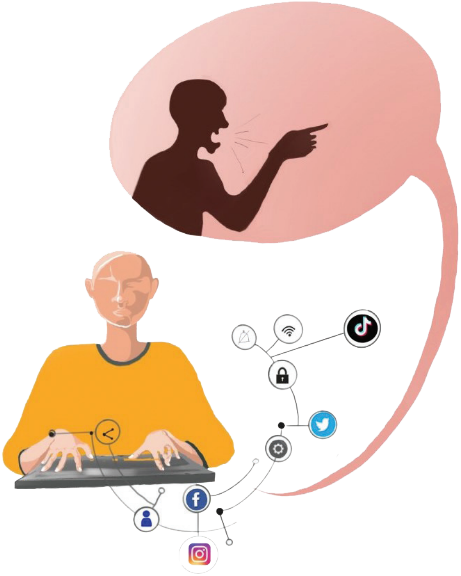
TO KEEP IN MIND: Intersectionality Within

We should recognise the intersectionality within women and gender diverse people to effectively address the issue. Identities of a person based on caste, ethnicity, class, religion, region, language, gender, disability, sexuality, etc. create unequal grounds for exclusion and experiences of marginalisation.



For example: a poor Dalit trans-woman politician from Madhes is more vulnerable to multiple forms of violence based on her different overlapping identities than a heteronormative, cisgender, high class, Nepali speaking, Brahmin woman from Kathmandu. So, we need to analyse gendered disinformation through these multiple identities as well.

IDENTIFYING GENDERED DISINFORMATION ONLINE



Gendered disinformation online is an extension of what already exists in the physical world. So, the root causes of such disinformation in the physical world, such as patriarchal mindset, socio-cultural norms and values, and other various forms of biases and prejudices against women and gender diverse people, are the same. Only the nature and forms of abuse are different. Some of these tactics – like astroturfing, deepfakes, etc, are not unique to online platforms and are often used in much broader disinformation campaigns, but online they have the potential to become more pervasive. Hence, it's important to identify different tactics of gendered disinformation online in order to counter them effectively. Some are discussed below:

TACTICS	DEFINITION	EXAMPLE
Astroturfing	The dissemination or amplification of content (including abuse) that gives an impression to have arisen organically from the grassroots level and spread. However, in reality, it is coordinated (often using multiple fake accounts) by an individual, interest group, political party, or organization.	*Short videos titled 'malai Sher Bahadur Deuba man parchha, kinabhane...' (I like Sher Bhadur Deuba, because...) were circulated on social media. Various well-known personalities were recorded praising Prime Minister Deuba in the video. An investigation by the news website Setopati found that those videos had originated from Deuba's Secretariat.*[10]

[10] Dhakal, K. (2021)

Catfishing	When someone creates a fake online identity to lure their target into a relationship and extract benefits, including financial benefits.	*In the Netflix documentary "The Tinder Swindler," a conman pretended to be the son of an Israeli-Russian diamond tycoon and scammed about $10 million (NPR 1,24,00,00,000 approx.) from multiple women.*
Concerned Trolling	When abusers pose as fans or supporters to make harmful and demeaning comments masked as constructive feedback, specially focused on appearance of women.	Comments such as "You should put more makeup; it brightens your face", "When you speak softly, it makes you more feminine and presentable."
Cyber Stalking	The persistent act of tracking target's internet use and following them around on online spaces, making unwanted contact through messages which can include threats, defamation, sexual harassment, or other actions to control or intimidate their target.	*A medical student was cyberstalked for six years through multiple fake Facebook accounts with messages that started as wooing, but after she didn't respond, included rape and death threats.*[11]
Deadnaming	Revealing a target's former name against their wishes in order to harm or humiliate them. It's a technique most commonly used against LGTBQIA+ community members who may have changed their birth names for different reasons, including to avoid physical danger or professional discrimination.	*Comedian Ricky Gervais faced criticism for deadnaming Caitlyn Jenner at Golden Globes 2016.*[12]

[11] Ghimire, A. (2021)
[12] THR (2016)

Deepfake	Creating fake images, audio, or video by using 'a form of artificial intelligence called deep learning' that appears real. These images, audio, and/or video mimic speech or facial expressions to make it look like someone has said or done something they haven't.	*Deepfake porn videos of Nepali actors Aanchal Sharma and Priyanka Karki were created and shared on porn sites.*[13]
Dogpiling (aka mob attacks)	When large groups of abusers collectively attack a target's online space through a barrage of threats, slurs, insults, and other abusive tactics with the intent to scare their target or make them retract their opinion.	Prominent Indian journalist Rana Ayyub received 50,000 abusive tweets in two days after she tweeted criticising the Saudi government's role in the Yemen war.[14]
Doxing	Publishing someone's personal information, such as their address, phone number and even their family members' details on online platforms as a call for others to harass, intimidate, extort, or stalk them.	*A woman of Kathmandu was bombarded with calls and messages from strangers after the perpetrator published her name, photographs, and phone number along with other information in a Facebook group.*[15]
Hate Speech	Threatening speech, expression or writing that expresses prejudice against a person, group, or their race, ethnicity, religion, gender identity or sexuality.	*Lawmaker Nabina Lama received hundreds of sexist and misogynistic comments in multiple social media platforms (Twitter, Facebook) for defending her colleague, then minister Yogesh Bhattarai, who had allegedly given a nod to a controversial land deal between the government and a business group.*[16]

[13] Bhetwal, A. (2022)
[14] Patterson, S. (2022)
[15] Acharya, N. (2019)
[16] PSA (2022)

Honey Trap	Approaching the target, usually in a seductive way, to gain information, money, or other vested interests.	*Kathmandu Metropolitan Police Crime Division arrested two men for allegedly using fake Facebook accounts with women's names and pictures to lure men and then blackmail them.*[17]
Identity Theft (Impersonation)	Stealing target's personal data to impersonate them on the internet or offline world.	*Indian actor Sunny Leone claimed that her permanent account number (PAN) was used by perpetrators for a loan fraud on Dhani App.*[18]
Lollipoping	Using terms, phrases or sentences that are meant to infantilise a person, especially a woman.	*Using words like "bunu", "nani", "maiya", "kanchhi", "timi ajhai bujhne bhayeki chhainau", "pachhi bujchhau", etc.*
Non-consensual dissemination of intimate images or videos	Publicizing someone's sexual images and videos (that might have been taken with or without permission) without their consent in order to cause them distress or embarrassment, with an intent to harm and/or as a form of revenge.	*A teenager's former boyfriend posted intimate pictures and videos of her in a private Facebook group after she broke up with him.*[19]
Outing	Disclosure of someone's sexuality, sexual orientation, or gender identity to the public without permission, which they have not yet chosen to do.	*An 18-year-old student died by suicide after he was outed by his roommate through Facebook livestreaming of his intimate moments with a man.*[20]

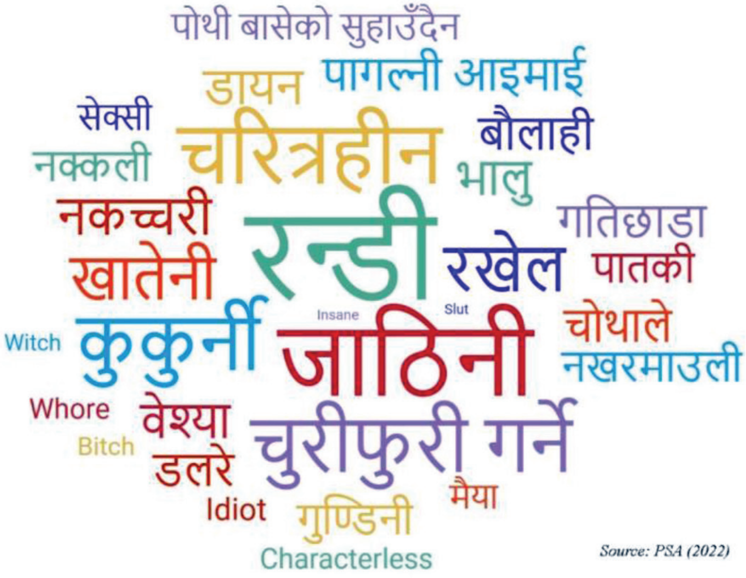
[17] The Himalayan Times (2016)
[18] Mihindukulasuriya, R. (2022)
[19] Satyal, U (2022)
[20] Pilkington, E. (2010)

Sextortion	A form of blackmail in which someone uses threats to elicit sexual favours from the victim.	*A businessman was arrested for allegedly drugging and raping a minor who was a participant in a beauty pageant organised by him in 2014. The survivor claims that the perpetrator forced her into sexual acts for six months by threating to release images/ videos taken during her abuse.*[21]
Shallow Fake	A method of manipulating media content using simple audio/video editing software, without making use of machine learning technology and algorithmic systems like in deepfakes.	*An altered video of politician Sujata Koirala was edited in such a way that she could be heard saying that Kalapani belonged to India. But it was taken out of context. She was merely repeating her statement, in which she had said Nepal could lease out Kalapani to India for 5-10 years because the country lacked access to the region.*[22]
Trolling	Making unnecessarily provocative and hostile comments with an intent to upset the target.	*Journalist and writer Amrita Lamsal is constantly tagged in tweets on subjects she generally speaks about. But if she has not reacted to a particular case, she is trolled with comments such as "Why are you silent on this issue?", "Not important enough for you, I guess."*
Threats	These are statements made with an intention to inflict pain, injury or other hostile actions upon a target. These include death threats and threats of physical violence, and for women, often threats of sexual violence.	*Publicly active women like journalist Binu Subedi and politician Nabina Lama are amongst others who have been targeted with threats of rape and physical violence.*

[21] Dhungana, S. (2022)
[22] Shiwakoti, S. (2020)

Zoombombing/ Googlebombing	This is an act of hijacking and disrupting a virtual meeting through the sharing of text, audio, or video. Generally, these attacks are conducted to disrupt the activities and silence the targets.	*On 16 May 2020, a Zoom conference of Female Foresters Nepal was hijacked and the participants were harassed with explicit sexual contents and verbal abuse by unknown and uninvited men.*[23]

Using these words is a form of gender- based violence!



Source: PSA (2022)

[23] Giri, K and Dangal, S (2020)

TACKLING GENDERED DISINFORMATION

The pervasive nature of gendered disinformation might be overwhelming, but it is preventable. There are actionable steps that can be taken by individuals, social media platforms, political parties, policymakers, and organisations to create a safer and healthier online environment for women and gender diverse people.

When it comes to tackling online gender-based violence and gendered disinformation, we must be social media literate and extra cautious about our digital security. The reasons behind it are:

- To avoid falling victim to GBV and disinformation.
- To avoid creating hostile environments for women and other marginalised groups.
- To avoid unintentionally committing online GBV crimes and spreading disinformation.

Hence, the following sections offer some tips on how to keep oneself safe digitally as well as tackle gendered disinformation on individual and institutional levels.

1. Take Precautions

Like locked doors are more effective than unlocked ones to prevent burglary; it's better to take measures to prevent online attacks. Online violence can happen in different shapes, sizes and forms, and through different platforms and technologies. Hence, being prepared and taking precautions to ensure one's digital security is important.

A. PROTECT YOUR DIGITAL DEVICES

- Devices (phone, laptop, notepad, etc.) have their own **privacy settings;** use them to manage and control your privacy and security.
- **Do not install unreliable apps** on your devices which can make your devices vulnerable to hacking and surveillance by state or non-state actors.
- **Install reliable antivirus** software for each device and update them regularly.
- **Use VPN (Virtual Private Network)** for secure and encrypted connection between your computer and internet.
- **Use encrypted USB sticks** to stay safe from harm in case you lose the USB sticks.
- To prevent others from tracking your location, **do not keep your geolocation ON** except when using the devices.

B. PASSWORD PROTECTION

- Make your phone, laptop and other digital devices **password protected**.
- **Use stronger passwords** for your social media accounts, email accounts and wifi network.
- **Do not use** your or your loved one's name, birth dates, or favourite places as passwords. These are easy for scammers to guess.
- **Do not use** the same password for multiple devices and accounts.
- **Do not share your password** with others.
- **Do not save passwords** of your accounts on any browser for easy access in your devices. It makes it easier for miscreants to access and exploit your privacy.
- You can **use password managers** such as KeePass (https://keepass.info/) to manage all your passwords safely.

C. STAYING SAFE IN A VIRTUAL WORLD	
DO	**DON'T**
✓ **Clear the cache, automatic form filling cookies, history** of your internet browsers at least once a week.	χ It is safer to **not link different social media** accounts with each other.
✓ **Choose 'do not remember'** option if you must use public Wi-Fi and devices to access your accounts.	χ To stay safe from hackers and avoid collection of your personal data by state/non-state actors**, do not use publicly available WiFi** on your devices. **Use Mobile Data** instead for safety.
✓ **Use Privacy settings** of social media platform to control who can connect with you, message you and view your posts. You can use **review option** to check any post before you share it on your account.	χ **Do not share your exact location** on social media. It makes you vulnerable to being tracked down.
✓ **Accept friend requests** only from people you know or have many mutual friends with.	χ **Do not share your personal details**, birth date, address, phone number, citizenship, bank details, or details of other important documents on social media. These details make you vulnerable to digital insecurity.
✓ Before using **online video-meeting platforms** like Zoom, Jitsi, etc, check their privacy and security settings to control access to the meeting and mute or remove disruptive participants.	χ **Do not share Meeting ID and Passcode** of online video-meeting platforms on social media.
✓ Choose safe messaging apps like Signal or WhatsApp that have **end-to-end encryption** in messages you exchange.	χ **Do not open** links of news/ information directly from social media. Open it on a different browser tab.
✓ **Use Proton mail, Tutanota email platforms, etc** that offer encryption for exchanging sensitive information.	χ **Do not click the links** shared with you without checking the title and the company, site, etc that it comes from.

2. Fact Checking is a MUST!

Fact checking is a crucial tool to counter gendered disinformation. It can prevent amplification and pervasiveness of inaccurate or deceptive information through social media sharing. Therefore, we should not share information without verifying, first. We must fact-check the information following the simple steps mentioned below:

Look at the sources:	▪ Does the image, graphics or post have credible sources such as recognised education institutions, legitimate companies, agencies, organisations, websites, or experts? ▪ **Do not share if it doesn't have reliable sources!**
Check the language:	▪ Viral posts often use sensational language for clickbait. They also often have grammatical errors. ▪ **Do not share information that uses emotional and incorrect language!**
Check the images/videos:	▪ Unreliable or inaccurate information contain photoshopped, distorted and often sexualised images/videos for clickbait. ▪ **Do not trust them or share them without verifying from multiple sources!**
Check other media:	▪ Check if other reliable media have reported on the issue. If they have not, wait. ▪ **Share only after verifying with at least three reliable sources!**
Act like a Journalist:	▪ Like a journalist, doubt everything, check and verify the information. ▪ **Do not trust each and every information available on social media and digital platforms!**
Check for objectivity:	▪ If authors or organisations sharing the information are known for representing a particular point of view, the arguments and facts might have been selectively chosen to support their viewpoints. ▪ **Be careful not to fall into this trap!**

Check Fact-checking sites:	▪ When in doubt, visit fact-checking websites which might have already fact-checked the information. ▪ http://southasiacheck.org/ ▪ https://nepalfactcheck.org/ ▪ https://www.factchecker.in/ ▪ https://www.altnews.in/ ▪ https://africacheck.org/

3. Steps to counter gendered disinformation

Gendered disinformation is not just the problem of women or gender diverse people. The gravity of the information disorder it creates impacts not only individuals but also institutions. So, we need to tackle it together, from different levels and in different capacities.

The National Democratic Institution (NDI) and other organisations working on gendered disinformation have some recommendations on how it can be countered at individual and institutional levels.[24] They are summed up in the following tables:

[24] NDI (2021b); Middlehurst, M (2021)

A. AT INDIVIDUAL LEVEL	
Don’t be silent!	▪ If you are targeted by gendered disinformation, you must speak out against it. ▪ **Debunking disinformation** is a way to deal with it.
Call out!	▪ If you witness any online GBV or gendered disinformation, **call it out on social media, then and there.**
Report it!	▪ Make sure to report it on the concerned online platform (they have their own harassment reporting mechanisms) and to relevant authorities.
Don’t share it!	▪ Sharing gendered disinformation amplifies hatred and disinformation. ▪ **Remember: Algorithm bias** on social media rewards and amplifies information for profit.
Contact fact checking websites	▪ Bring gendered disinformation to their notice.
Follow up!	▪ Once you report to the tech companies owning the social media, authorities, political parties, or perpetrators’ affiliated organisations, **keep following up on the progress** of the issue.
Continue to educate yourself!	▪ **Keep learning about gender stereotypes and biases** and ways to mitigate them.

Does your working space offer support system to deal with online GBV and gendered disinformation?

TO KEEP IN MIND!
Research shows that majority of women do not know where to go for digital safety support in their working spaces.

B. AT INSTITUTIONAL LEVEL	
Training and Awareness Sessions	▪ Institutions like political parties, media houses, and civil society organisations must **organise training and awareness sessions** for their members, journalists, and staff **on recognising gendered disinformation and countering them.** ▪ Create awareness on difference between freedom of expression and gendered disinformation.
Go To Desk	▪ Must have a dedicated **'go to desk'** that provides support and services needed to deal with gendered disinformation, like psychosocial counselling and legal assistance, and helps the victim report the issue.
'Code of conduct'	▪ Should formulate a **'code of conduct'** to curb the spreading of gendered disinformation and to counter hate speech, dis/mis/mal-information.
Take a public stance	▪ **Take a public** stance against gendered disinformation and GBV in political party manifestoes and institutional Gender Equality and Social Inclusion (GESI) policies or strategies.
Monitoring Team	▪ Have a committed **team to monitor, report and act against** gendered disinformation and GBV.
Service Announcement	▪ Media should **develop service announcements** to counter gendered disinformation and adopt a 'code of conduct' for covering women and gender diverse people.
Online monitoring mechanism	▪ Traditional media should have **online monitoring mechanisms to regulate** their social media channels (Facebook, YouTube, Twitter etc) and censor defamatory or sensitive content targeted towards women and minorities.
Show solidarity	▪ Institutions must **publicly denounce** gendered disinformation attacks and **show solidarity to support targets.**
Support Networks	▪ Develop **support networks** of women, media monitoring groups, journalists, and civil society organisations working for the rights of women and marginalised groups to further examine disinformation and counter them.

Rules and Regulations	▪ Legislatures should **adopt rules** against creating and sharing of gendered disinformation.
Legal recourse	▪ Advocate for **legal recourse** against gendered disinformation in both physical and virtual worlds.
Engage with online ‘influencers’	▪ To help address gendered disinformation with **counter messaging** and to create awareness amongst voters.
Invest in Fact-Checking efforts	▪ Encourage and invest in **Fact-Checking efforts** made by individuals, groups, and organisations.
Encourage women	▪ **Encourage women to be active on social media** as political and civil careers requires them to be online.

4. Reporting Online Violence

PEN America on its ‘Online Harassment Field Manual’ recommends assessing the threat level of the online violence to address it effectively. The manual recognises two categories of online harassment: pervasive and severe.

Pervasive online violence such as trolling, concerned trolling, lollipopping, etc. can be dealt with by using simple social media features like muting (notifications and posts from the muted account are not shown on your social media timeline), restricting (not allowing commenting, sharing or viewing of your post by the restricted account), and blocking (the account is blocked from interacting with you, the person can see you have blocked them). These features help in controlling who can connect, view, or interact with you on social media. Almost all social media platforms have these options in their Privacy settings. If the abuse is persistent and the threat level intensifies, you should consider reporting the perpetrator and the contents of abuse to the social media platforms concerned, seek support from trusted online groups, and mobilise your online community to respond with strategic counteraction.

Severe online violence such as deepfake, identity theft, sextortion, death or rape threats, doxing etc. have serious consequences. Therefore, if you are the target of these online abuses, you should consider the following things:[25]

- Involving local law enforcement
- Consulting a lawyer
- Informing your employer
- Reaching out to friends and family
- Reaching out to organisations working on Gender Based Violence or human rights

Documenting the Violence: Reporting online violence requires submitting detailed information on the type of violence that has occurred. So, documenting the abuse as proof is crucial. Here are some tips:[26]

Documenting the Violence	
Screenshots	▪ Most smartphones, computers, tablets, etc. have a feature for capturing images directly from the screen (screenshots). ▪ Use screenshot feature to keep records of online harassment in emails, messages, phone calls, etc. ▪ Keep them safe on external USB sticks. ▪ Print of screenshots are important for hard-copy documentation when filing a police report.
Logging Online Harassment	▪ Create a log to keep detailed and specific information on the online harassment that you are facing. The log must include: 1. **Date and Time** 2. **Type of electronic communication** (email, direct message, posted image, phone call, social media comment, etc) 3. **Location** (name of the app or website) 4. **Nature of the online incident** (doxing, death threat, casteist or racist attack, sextortion, or anything else) 5. **Details of the perpetrator** (including name, email ID, online profile or handle, etc)

[25] PEN America (2022)
[26] Ibid

What to Document	▪ **Emails:** Emails can help in tracking down a sender. So, be sure to save the header that contains the **IP address**. **Do not forward the original email** to anyone as it can make you permanently lose the original IP address. **Copy and paste** the email content and share instead. ▪ **Messages sent on social media platforms:** Since abusive contents on social media can be removed by the original user or platform, it's important to **save screenshots and hyperlinks** where possible to keep a record of the harassment. ▪ **Texts and harassing phone calls:** Don't forget to take screenshots of the text messages and available contact information of the sender. Keep the details of threatening phone calls and texts in the log (ref. Logging online harassment).
Remember	▪ **Document all relevant evidences, not just the evidence that supports you**. If your reactions have contributed in any way to the escalation of harassment, document that too. Not documenting all aspects of harassment can harm you if you ever go to the court. T**o report the abuser and seek justice, you don't have to prove that you have reacted perfectly.** ▪ You don't have to do it all alone. You can **seek support from trusted friends and family members** to help you in documenting the abuse.

Reporting the violence:

Where	Contact Details
Cyber Bureau, Nepal Police Chittadhar Marg, Kathmandu	Mobile number: **9851286770** Phone Number: **014219044** Email: cyberbureau@nepalpolice.gov.np
National Women Commission Prithvi Path, Kathmandu	Helpline: **1145**
Local units in municipality/rural municipality	Judicial Committee

Where to complain on social media platforms:

Facebook	Substantive info on reporting different scenarios: https://t.ly/YzOe Report an imposter page of a public figure: https://t.ly/t7rm How to report things, broken down by different types of posts: https://t.ly/wlQZ How to mark a post as false news: https://t.ly/gLaZ
Twitter	General overview of report violations: https://t.ly/Etfe How to report a tweet, abusive account, or individual message: https://t.ly/8BX3 Report an impersonation account: https://t.ly/X3TI Report spam instructions: https://t.ly/qo65

5. Take steps for self-care

Online violence can be overwhelming and harmful for your overall well-being: psychological, physical, and economic. So, taking care of your wellbeing should be prioritised.

Some of the actions you can take for self-care while dealing with online gender-based violence including gendered disinformation are discussed below:

Things to remember	▪ **This is not your fault**. ▪ There are ways to deal with it. You are not alone.
Limit your exposure	▪ **Limit the time you spend on social media**; have a fixed time for your online activities. ▪ **Turn off your phone or keep it in silent mode or mute notifications**, especially at night. ▪ **You don't have to immediately react** to some of the perverse online harassment.
Keep a journal	▪ Writing about your online experience **can be helpful in processing your trauma** and can give you important distance from the experience.
Do Physical Exercise	▪ Physical exercise **can help release stress** related to the emotions.
Head into nature	▪ Spending time in nature with fresh air, greenery and taking long walks **can be therapeutic.**
Do the things you love	▪ **Focus on the things that you love**: reading, writing, watching movies, listening to music, cleaning, cooking, eating your comfort food and drinks, playing with pets or kids, etc.
Be with people you love	▪ Spend time with the people who care about you, love you, support you and **help you in staying positive.**
Donate or volunteer	▪ Donate or volunteer with the organisation that are working against online violence. ▪ Donating or volunteering **can be a powerful and cathartic way to process one's abuse.**

WORKS CITED AND REFERENCES

Acharya, N. (2019) 'Nepal's rape culture has gone online – and our laws are dismal'. *The Record*. 4 August. Available at: https://www.recordnepal.com/nepals-rape-culture-has-gone-online-and-our-laws-are-dismal (Accessed: 16 March 2022)

Bhetwal, A. (2022) 'How to avoid 'shallowfake' and 'deepfake' that impact election?' Himal Khabarpatrika. 13 April. [in Nepali] Available at: https://www.himalkhabar.com/news/129176 (Accessed: 25 April 2022)

CEPPS (2021) *Understanding the gender dimensions of disinformation.* Consortium for Elections and Political Process Strengthening. Available at: https://counteringdisinformation.org/node/13/ (Accessed on 18 July 2022)

Dhakal, K. (2021) 'PM Deuba's Secretariat created 'propaganda' videos'. *Setopati*. 5 July. Available at: https://www.setopati.com/politics/245260 (Accessed: 27 April 2022)

Dhungana, S. (2022) 'Manoj Pandey, a beauty pageant organiser accused of rape, in police custody'. *The Kathmandu Post.* 22 May. Available at: https://kathmandupost.com/national/2022/05/21/alleged-rapist-in-police-custody (Accessed: 25 May 2022)

Ghimire, A. (2021) 'Online harassment rife but largely ignored as system fails to recognise it'. *The Kathmandu Post.* 6 December. Available at: https://kathmandupost.com/national/2021/12/06/online-harassment-rife-but-largely-ignored-as-system-fails-to-recognise-it (Accessed: 15 March 2022)

Giri, K and Dangal, S. (2020) 'Woes of Women Foresters', *The Rising Nepal.* 07 August. Available at: https://risingnepaldaily.com/detour/woes-of-women-foresters (Accessed: 15 February 2022)

Heinrich-Boll-Stiftung European Union (2021) *Gendered disinformation: How should democracies respond to this threat?* 9 June. [Online Video]. Available at: https://www.youtube.com/watch?v=10dhgc1oD1o&list=WL&index=18&ab_channel=Heinrich-B%C3%B6ll-StiftungEuropeanUnion (Accessed: 27 January 2022)

Middlehurst, M. (2021) *Violence Against Women in Politics: Online Violence and Disinformation* [PowerPoint Presentation]. December 2021. National Democratic Institute.

Mihindukulasuriya, R. (2022) 'Actor Sunny Leone claims identity theft, PAN details allegedly used for fintech loan fraud'. *The Print.* 17 February. Available at: https://theprint.in/india/actor-sunny-leone-claims-identity-theft-pan-details-allegedly-used-for-fintech-loan-fraud (Accessed 17 March 2022)

NDI. (2021a) *Addressing Online Misogyny and Gendered Disinformation (w/ Neema Iyer and Nina Jankowicz)*. 27 September. [Online Video]. Available at: https://www.youtube.com/watch?v=Ue56U9fxY_w&list=WL&index=19&ab_channel=NationalDemocraticInstitute (Accessed: 20 January 2022)

NDI. (2021b) *Addressing Online Misogyny and Gendered Disinformation: A How-To Guide.* National Democratic Institute.

NDI. (2021c) *Tweets that chill: Analyzing Online Violence Against Women in Politics.* National Democratic Institute. Available at: https://www.ndi.org/sites/default/files/NDI%20Tweets%20That%20Chill%20Report.pdf (Accessed 18 July 2022)

NepalFactCheck.org (2022a) 'Setopati's detail on Deputy Mayoral candidates of Kathmandu Metropolitan City is wrong'.4 May. Available at: https://nepalfactcheck.org/2022/05/ktm-municipality-setopati-news/ (Accessed: 11 May 2022)

NepalFactCheck.org (2022b) 'What is the fact behind complaint at CIAA against deputy mayoral candidate Sunita Dangol?'. 3 May. Available at: https://nepalfactcheck.org/2022/05/sunita-dongol/ (Accessed: 11 May 2022)

Patterson, S. (2022) 'Rana Ayyub – The Perfect enemy for Narendra Modi's 'Troll Army''. Women in Journalism. 4 March. Available at: https://womeninjournalism.co.uk/rana-ayyub-the-perfect-enemy-for-narendra-modis-troll-army-by-sally-patterson/ (Accessed: 30 April 2022)

PEN America (2022) *Online Harassment Field Manual.* Available at: https://onlineharassmentfieldmanual.pen.org/ (Accessed: 10 March 2022)

Pilkington, E. (2010) 'Tyler Clementi, student outed as gay on internet, jumps to his death'. *The Guardian.* 30 September. Available at: https://www.theguardian.com/world/2010/sep/30/tyler-clementi-gay-student-suicide (Accessed: 10 March 2022)

PSA (2022) *Analysis of Gendered Violence in Media Against Women in Politics in Nepal.* Panos South Asia, Kathmandu.

Satyal, U. (2022) 'More girls becoming victims of revenge porn'. *The Himalayan*

Times. 4 January. Available at: https://thehimalayantimes.com/nepal/more-girls-becoming-victims-of-revenge-porn (Accessed: 10 April 2022)

Shiwakoti, S. (2020) 'Viral video clips involving Sujata Koirala were manipulated to create controversy'. *South Asia Check*. 21 May. Available at: https://southasiacheck.org/fact-check/viral-video-clips-involving-sujata-koirala-were-manipulated-to-create-controversy/ (05 May 2022)

Thapa, M. (2002) 'Patriarchy, female freedom Shrisha Karki'. *Nepali Times*. 06 – 12 December, Issue 122. Available at: http://archive.nepalitimes.com/news.php?id=4364 (Accessed: 12 March 2022)

The Himalayan Times (2016) 'Cyber crime incidents on rise'. *The Himalayan Times*. 21 February. Available at: https://thehimalayantimes.com/kathmandu/cyber-crime-incidents-rise (Accessed 20 March 2022)

THR (2016) 'Golden Globes: Ricky Gervais Defends Caitlyn Jenner Joke'. *The Hollywood Reporter*. 12 January. Available at: https://www.hollywoodreporter.com/news/general-news/ricky-gervais-defends-caitlyn-jenner-joke-golden-globes-trans-854902/ (Accessed 17 March 2022)

Wardle, C. (2019) *First Draft's Essential Guide to Understanding Information Disorder*. First Draft.

Yami, H. (2021) ''Hisila': This memoir tells the story of the Leftist revolutionary who became Nepal's first lady'. *Scroll.in*. 9 June. Available at: https://scroll.in/article/997004/hisila-this-memoir-tells-the-story-of-the-leftist-revolutionary-who-became-nepals-first-lady (Accessed: 10 March 2022)

ADDITIONAL RESOURCES

Organisation	Website
Body & Data	https://bodyanddata.org/
Digital Rights Nepal	https://digitalrightsnepal.org/
First Draft	https://firstdraftnews.org/long-form-article/understanding-information-disorder/
Loom Nepal	https://taannepal.org.np/
NepalFactCheck.org	https://nepalfactcheck.org/
PEN America	https://onlineharassmentfieldmanual.pen.org/
South Asia Check	http://southasiacheck.org/
Tactical Tech	https://kit.exposingtheinvisible.org/en/index.html

ACKNOWLEDGEMENTS

This handbook draws inspiration from similar campaigns across the world that strive to create a safer and healthier online environment for women and gender diverse people to engage and benefit from the platforms and opportunities that the internet and technologies provide. The resources from National Democratic Institute (NDI), First Draft, PEN America, South Asia Check, Body & Data, Loom Nepal, campaigns such as #ShePersisted, #NotTheCost were particularly helpful in the framing of this resource.

This handbook would not be possible without the valuable support from the Panos South Asia team and reviewers. In particular, Smita Magar played a crucial role in researching, analyzing and adapting the handbook content for a Nepali audience. We would like to specially thank National Democratic Institute (NDI) and the USAID for their support and engagement throughout the process.

All social media materials have been cited from accounts or posts in the public domain.

ABOUT PANOS SOUTH ASIA (PSA)

Panos South Asia (PSA) encourages and facilitates public debate on a wide range of issues. It seeks to enable diverse opinions, ideas and theories through media to be included in the debate on governance and development to make societies more inclusive, democratic, and just. Since October 2021, PSA has embarked on identifying the phenomena of disinformation, using a gender sensitive lens to locate examples of misogyny in the online public sphere in Nepal. It aims to reduce the level of harm caused due to the spread of deliberate lies and hate speech against women politicians; to create awareness and build capacity of local stakeholders to better understand and tackle the latest trends and techniques of online gendered disinformation; and to ensure citizens access to the necessary facts to make more informed political choices during elections.

NDI
NATIONAL DEMOCRATIC INSTITUTE FOR INTERNATIONAL AFFAIRS

USAID
FROM THE AMERICAN PEOPLE

PANOS
SOUTH ASIA