



DIGITAL LITERACY AND ONLINE SAFETY TOOLKIT

*For Women Human Rights Defenders (WHRDs)
and Women Leaders in Kenya*

June 2026

TABLE OF CONTENTS

Background	IV
Glossary of Terms	V
MODULE 1	
INTRODUCTION TO DIGITAL LITERACY AND ONLINE SAFETY	1
1.1 How to Identify and Understand Digital Threats	1
1.2 Common Adversaries facing WHRDs	2
<i>Activity: How to Build Your Threat Model</i>	2
MODULE 2	
KEEPING YOUR DEVICES AND ACCOUNTS SAFE	
2.0 Screen Lock and Protection	4
Updating Your Devices and Apps	4
Safe Charging and Connections	4
<i>Danger Signs on your Device</i>	4
2.1 Two-Factor Authentication (2FA) – Extra Protection for Devices and Accounts	5
Priority Accounts to Protect with 2FA	5
<i>Activity: Practice How to Create a Strong Password</i>	
MODULE 3	
SOCIAL MEDIA SAFETY AND PRIVACY	6
3.1 Privacy Settings on Social Media Platforms	6
3.2 Staying Safe while using Social Media	6
Location Awareness	6
Network Exposure	7
Spotting Fake Accounts and Phishing :Red flags and what to do	7
If You Think Your Account Has Been Hacked	7
3.3 Understanding Data Privacy on Social Media	8
What information is collected?	8
How to protect your privacy?	8
MODULE 4	
STAYING SAFE FROM ONLINE HARM – HARASSMENT,DOXXING AND SURVEILLANCE.	9
4.1 Online Harassment	9
Prevention Strategies	9
If Harassment Occurs	9
If You Receive A Threat of Physical Violence	10

4.2 Doxxing	10
How to Protect Yourself	10
4.3 Digital Surveillance	10
Emergency Contacts	10

MODULE 5

SECURE COMMUNICATION AND TOOLS

5.1 Messaging Apps: What You Should Know	12
5.2 Getting Started with Signal	13
5.3 Using a Virtual Private Network (Extra Internet Protection)	
Secure Ways To Store And Share Files Online	13

MODULE 6:

LEGAL FRAMEWORKS AND REPORTING MECHANISMS IN KENYA

6.1 How and Where to Report	14
6.2 Documenting Incidents for Legal Purposes	16
Know Your Rights If Contacted by Police	

MODULE 7

BUILDING A SAFE DIGITAL PRESENCE AND ADVOCACY

7.1 Strategic Identity Management	17
7.2 Effective and Safe Digital Advocacy	17
Building Audience and Visibility Safely	17
Content Strategy for High-Risk Advocacy	18
Coalition and Solidarity	18
7.3 Self-Care and Digital Wellbeing	19
Building a Resilient Digital Strategy	

MODULE 8

DISABILITY INCLUSION IN DIGITAL SPACES

8.1 Common Challenges and Practical Solutions by Disability Type	19
For women with visual impairments	19
For women with hearing impairments	19
For women with physical disabilities	19
For women with cognitive or psychosocial disabilities	20
8.2 How to make digital spaces more inclusive	20
8.3 Respect and Safety for Women with Disabilities Online	20
8.4 Quick Checklist Before You Post Online	21

Background

Digital technologies have become indispensable tools for civic engagement, human rights advocacy, journalism, political participation, and community organising in Kenya. However, these opportunities have been accompanied by growing digital risks, particularly Technology-Facilitated Gender-Based Violence (TFGBV), online harassment, surveillance, misinformation, and cyber threats that disproportionately target Women Human Rights Defenders (WHRDs), women leaders, journalists, and other individuals with a visible public presence. These attacks are often designed to intimidate, silence, undermine credibility, and discourage participation in public life, especially during elections, civic actions, and other politically sensitive periods.

While Kenya continues to strengthen its legal and policy framework on digital rights and online safety, many frontline actors still face significant challenges in preventing, responding to, and recovering from digital threats. Limited awareness of digital security practices, evolving technologies, and inconsistent enforcement of existing protections leave many vulnerable to online abuse, privacy violations, and coordinated attacks. As digital spaces continue to evolve, so too do the tactics used by perpetrators, making practical digital resilience an essential component of effective advocacy and leadership.

Recognising these emerging challenges, the Community Advocacy and Awareness Trust (CRAWN Trust), with support from the African Women's Development Fund (AWDF), is implementing the Safe Spaces, Strong Voices project. One of the project's initiatives was a national Gap Analysis of Technology-Facilitated Gender-Based Violence in Kenya. The findings underscore the urgent need for practical, accessible, and context-specific capacity building that equips frontline actors with the knowledge and skills to safely navigate digital spaces while continuing their important work.

This Digital Literacy and Online Safety Toolkit has therefore been developed as a practical resource for Women Human Rights Defenders, women leaders, journalists, and civil society actors. It provides step-by-step guidance on identifying digital risks, protecting devices and online accounts, responding to online harassment, communicating securely, understanding legal protections, conducting safe digital advocacy, promoting disability-inclusive digital practices, and developing personalised digital safety plans. Through its eight learning modules and Digital Safety Checklist, the toolkit aims to strengthen digital resilience, enhance personal and organisational security, and enable users to continue exercising their rights to freedom of expression, participation, and advocacy in increasingly complex digital environments.

We hope this toolkit will serve as a practical and accessible resource, encouraging safer digital practices and supporting secure and meaningful online engagement. CRAWN Trust remains committed to promoting inclusive, rights-based digital spaces that enable individuals to participate, lead, and advocate safely and effectively.

Daisy Amdany
Executive Director
CRAWN Trust

Josephine Marura M.
Consultant
Gender Equality & Disability Inclusion Expert

Glossary of Terms

Term	Definition
2FA (Two-Factor Authentication)	A security method requiring two forms of verification typically your password plus a code from an app or SMS.
Cyber Bullying	Bullying that takes place over digital devices, involving repeated hostile behavior such as name-calling, spreading rumors, or exclusion in online spaces.
Cyber Stalking	Persistent monitoring, tracking, or unwanted contact through digital means that causes fear or distress. This can include repeated messages, location tracking, or surveillance.
Digital Footprint	The trail of data a person leaves behind when using the internet, which can sometimes be exploited in cases of TFGBV.
Digital Surveillance	The use of technology to monitor someone's activities, communications, or location without their consent. This can occur in intimate relationships or through spyware and tracking tools.
Doxxing	Publishing someone's private personal information such as contact information or home address online without consent to expose or incite harassment against them.
End-to-end encryption (E2EE)	A communication method where only the sender and recipient can read messages, not the platform or any third party.
EXIF data	Metadata embedded in photos, often including GPS location, camera model, and date/time. Can inadvertently reveal your location.
Impersonation	Creating fake accounts or using someone else's identity online to deceive others, damage their reputation, or carry out abuse in their name.
IP Address (Internet Protocol address)	It is a unique number assigned to a device when it connects to the internet or a local network which works like a digital home address so that data knows where to go and where it came from.
Juice Jacking	A type of cyberattack where a public USB charging station (like those in airports, malls or hotels) is tampered with so it can steal data from your device or install malware while it's charging.
Online Harassment	Repeated or severe abusive behavior carried out on digital platforms, including insults, threats, or degrading comments intended to intimidate or silence someone.
OTP (One-Time Password)	A single-use security code sent to your phone, email, or authentication app to confirm that it is really you trying to access an account or complete a transaction.
Platform Accountability	The responsibility of technology companies to prevent, address, and respond to harmful content and behavior on their platforms.
Phishing	A deceptive attempt via email, message, or fake website to trick you into revealing passwords or clicking harmful links.

Spyware	Malicious software secretly installed on a device to monitor communications, location, or activities without the owner's knowledge.
Survivor-Centered Approach	A way of responding to violence that prioritizes the rights, safety, dignity, and choices of the person who has experienced harm.
Threat model	A personalized assessment of who might want to harm you digitally, what they might do, and what steps to take to protect yourself.
Trolling	Deliberately provoking or upsetting someone online by posting inflammatory, offensive, or misleading content, often to get a reaction.
VPN (Virtual Private Network)	A service that encrypts your internet traffic and hides your IP address, protecting your browsing from surveillance on public networks.
WHRD (Women Human Rights Defender)	A woman who acts to promote or protect human rights, often facing gender-specific risks as a result.
TFGBV (Technology-Facilitated Gender-Based Violence)	Any act of violence committed, assisted, or amplified through digital technologies (such as phones, social media, or online platforms) that targets a person based on their gender or disproportionately affects them because of it.
USB protector (often called a USB data blocker)	A small device that you plug between your charging cable and a USB port to allow power to flow but block any data transfer reducing the risk of hacking or data theft.

MODULE 1

INTRODUCTION TO DIGITAL LITERACY AND ONLINE SAFETY

Today, many Women Human Rights Defenders (WHRDs) use smartphones, social media platforms and the internet to share information, speak out and support their communities. These digital tools make it easier to connect, learn, and advocate for change. However, being online can also come with risks. Women may face online harassment, scams, false information or misuse of their personal data. These risks can affect safety, confidence, and wellbeing.

Digital literacy means having the skills to use digital tools like smartphones, Apps and the internet in a safe and useful way. It also includes knowing how to tell what information is true, how to protect your personal details and how to communicate responsibly online. In addition to staying safe, it's important to build confidence in using digital tools effectively.

- **Understanding apps and tools:** Learn what common apps (e.g. messaging, email, browsers) are used for and how to navigate them.
- **Finding information:** Practice searching online and identifying reliable sources
- **Evaluating content:** Not everything online is true, learn to question and verify information before sharing.
- **Managing data and storage:** Know how to save, delete, and organize files, photos and messages.
- **Communicating online:** Use clear, respectful communication and understand basic digital etiquette.

Digital literacy is not just about safety, it's about confidently using technology to access information, communicate, and participate online.

Online Safety is about protecting yourself when using digital platforms. This includes using strong passwords, keeping your personal information private and knowing what to do if you experience online abuse.

This toolkit is therefore designed to support WHRDs to:

- Use digital tools with confidence
- Stay safe while online
- Protect their information, identity and community
- Prevent and respond to online risks and challenges

1.1. How to Identify and Understand Digital Threats

Before adopting any security tool, you need to understand your specific situation and potential risks. This is called a threat model and it helps you focus your energy where it matters most. A **Threat Model** is a structured way of thinking about who might want to harm you, what they want and what they are capable of.

Five key questions guide the understanding of this process:

<i>What do you want to protect?</i>	Contacts, documents, location, communications, identity.
<i>Who might want to access it?</i>	Stalkers, abusive partners, state actors, online trolls, criminal networks, employers, Political opponents
<i>How relevant/serious is the threat?</i>	Not every risk has equal threats. Prioritize the most realistic threats for your situation.
<i>What are the consequences if I fail at mitigating risks?</i>	What is at stake: physical safety, loss of job, legal consequences, exposure of sources, etc.
<i>How much am I willing to invest?</i>	Balance protection with usability. The best tool is one you will actually use consistently.

1.2 Common Adversaries facing WHRDs

- State actors and security forces: surveillance, account monitoring, phone interception.
- Online mobs, trolling and coordinated online harassment campaigns often triggered by public advocacy: doxxing, cyberbullying.
- Abusive or controlling intimate partners: location tracking, account takeover, intimate image abuse.
- Criminal networks: phishing, extortion, financial fraud.
- Employers or institutions: retaliation against whistleblowers or activists.

1.3 Misinformation & Disinformation: How to Spot False Information

Women Human Rights Defenders often receive and share information quickly. Being able to identify false or misleading content is essential.

What's the difference?

- **Misinformation:** False information shared without intent to harm
- **Disinformation:** False information shared deliberately to mislead or cause harm

How to check if information is reliable

- **Check the source clearly:** Make sure the information comes from a trusted organization, media house, or official page. Be aware that some fake accounts or websites copy the names and logos of real institutions e.g. media houses to spread false information and confuse people.
- **Look for confirmation:** Are other credible sources reporting the same information?
- **Check the date:** Old information is sometimes reshared as if it is new.
- **Watch for emotional language:** Content designed to provoke fear or anger may be misleading.
- **Verify images/videos:** Visuals can be edited or taken out of context.

Before You Share Any Information Online

BEFORE YOU SHARE ANY INFORMATION ONLINE

A PAUSE TODAY PREVENTS MISINFORMATION TOMORROW.

Not everything online is true. Take a moment to check facts, consider the source, and think before you share.

“A few seconds of skepticism can save countless others from misinformation.”

1 PAUSE AND VERIFY.

Don't let impulse outrun accuracy. Take a moment to stop and think.

2 ASK: WHO CREATED THIS AND WHY?

Check the source. What's their purpose? Are they biased, selling something, or informed?

3 CHECK THE FACTS.

Look for evidence. Cross-check with reliable, trusted sources. Don't rely on just one post or screenshot.

4 WHEN IN DOUBT, DON'T SHARE.

It's okay not to share. You could be stopping rumors, panic, or harm.

YOU HAVE THE POWER TO PROTECT TRUTH. PEOPLE. COMMUNITY.

Share wisely. Think critically. Build a better internet—together.

BE INFORMED. BE THOUGHTFUL. BE THE DIFFERENCE.

Activity: How to Build Your Threat Model

- Write down three assets you want to protect (e.g. your location, your sources, contacts, documents).
- Identify who is most likely to try to access each one of the assets.
- Rate each threat: Low/Medium/High risk.
- Identify one action you can take for each high-risk item.

Key Message : To make sure that digital spaces are safe, inclusive, and empowering for all women, including Women With Disabilities.

MODULE 2

KEEPING YOUR DEVICES AND ACCOUNTS SAFE

2.0 This module shows you how to protect your devices (laptops and smartphones) and accounts. These devices are gateways to everything else. Therefore, protecting them is the foundation of digital/online safety

Screen Lock and Protection

- Use a strong screen lock by using a 6+ digit PIN or a strong passphrase with unique characters.
- Avoid patterns and fingerprints in case you may be forced to unlock your device.
- Do not share your passwords with others or place it where others can find it.
- Make sure your screen locks itself automatically after 30 seconds of inactivity.
- Most devices will protect your information when you set a password, so always keep this feature turned on.

Updating Your Devices and Apps

- Enable automatic updates for your devices and all apps. Updates always help to fix problems and keep your devices safe.

Delete apps you no longer use and when installing new apps, check the permissions and privacy settings carefully to avoid sharing unnecessary personal information like your contacts, live location or photos.

Safe Charging and Connections

- Avoid public USB charging stations especially in airports or malls (risk of 'juice jacking'). Use your own charger when possible. If you must use public charging, use a USB Protector if available.
- Turn off Bluetooth and Wi-Fi when not in use.
- Be careful when using public Wi-Fi. Avoid sharing personal information when connected

Danger Signs on your Device

- Your battery is draining very fast, even when you are not using your phone.
- Your phone becomes hot even when it is idle (not in use).
- Your mobile data is being used up faster than usual.
- You see Apps on your phone that you did not install.
- Your camera or microphone turns on by itself without you using it

2.1 Two-Factor Authentication (2FA) – Extra Protection for Devices and Accounts

A security method requiring two forms of verification, typically your password plus a verification OTP code sent to an app, SMS or email. Even if someone knows your password, they still cannot access your account without the second code or approval.

There are different types of 2FA:

SMS Code/Text Message	Basic Option	A code is sent on your phone via a text message. It can be risky, though, if someone has taken control of your SIM card. Avoid high-risk accounts.
Authenticator App	Safer Option	Apps like <u>Google Authenticator</u> , <u>Authy</u> , or <u>Aegis Authenticator</u> generate time-based codes as a One Time Password (OTP) for your devices and accounts. This is a strong and recommended option.
Security Key	Strongest Option	A small physical device (like a USB) that you must plug in or tap to log in. This gives the highest level of protection

Priority Accounts to Protect with 2FA

PRIORITY ACCOUNTS TO PROTECT WITH 2FA

Turn on Two-Factor Authentication (2FA) for the accounts that hold your personal, financial, and important information.

- 01 EMAIL ACCOUNTS**
(Gmail, Outlook) – These are often the master key to all other accounts.
- 02 SOCIAL MEDIA PLATFORMS**
Twitter/X, Facebook, Instagram, LinkedIn, TikTok.
- 03 MESSAGING APPS**
WhatsApp, Signal and Telegram.
- 04 ONLINE BANKING & MOBILE MONEY**
MPESA, bank apps.
- 05 CLOUD STORAGE**
Google Drive, Dropbox, iCloud.

WHY 2FA?
Even if someone gets your password, 2FA stops them from getting in.

TIP:
Use an authenticator app (Google Authenticator, Authy) for the strongest protection.

SECURE TODAY. STAY PROTECTED TOMORROW.

YOUR ACCOUNTS. YOUR DATA. YOUR SECURITY. TAKE CONTROL.

#SecureSmart

Activity: Practice How to Create a Strong Password

Learn how to create and use strong passwords to stay safe online.

- Discuss common passwords people use and why they are risky and learn to:
 - Avoid names, birthdays, or “123456”
 - Use long passphrases (e.g. 3–4 random words with unique characters and/or numbers *57Yellow!Lion.Runs.Fast)
 - Use a different password for each account.
 - Use a password manager like Bitwarden (free)
- Practice how to create your own strong password using words, numbers, and symbols.
- Reflect and share what you will change about your passwords

Key Message: Use long, unique passwords and do not share them with others.

MODULE 3

SOCIAL MEDIA SAFETY AND PRIVACY

Social media is a powerful tool for advocacy, mobilization, and community building, but it is also where WHRDs and women leaders face the most visible threats. This module helps you use these platforms confidently while minimizing exposure.

3.1 Privacy Settings on Social Media Platforms

Social Media Platform	Privacy Settings
Facebook/Meta	Set your posts to “Friends only,” hide your phone number and email address, turn off face recognition, review app permissions, and enable login alerts. Remember that even people in your circle may have hacked accounts, which can expose your information to criminals.
Instagram	Switch your account to private so only approved followers can see your content. Control who can view your stories, turn off location tagging on posts and regularly review and remove any third-party apps connected to your Instagram account that you do not trust or no longer use.
Twitter/X	Protect tweets for more privacy. Turn off location sharing. Limit who can find you using your phone or email.
WhatsApp	Hide Last Seen and profile photo from everyone except contacts. Enable two-step verification. Turn off automatic media downloads. Disable read receipts for sensitive work.
TikTok	Set account to private. Disable location sharing. Turn off Personalized Ads. Control who can duet, stitch, or comment.
LinkedIn	Control who sees your connections list. Turn off activity broadcasts when updating your profile. Limit profile visibility carefully if your work is sensitive.

3.2 Staying Safe while using Social Media

Location Awareness

- Do not share where you are in real time.
- Avoid posting your home address or daily routine publicly.
- Post photos only after you have left a place.
- Remove hidden location details from photos before sharing.

Network Exposure

- Be cautious about publicly identifying colleagues, sources or vulnerable individuals in your posts.
- Do not accept friend or follower requests from unknown accounts without verification
- If your work is sensitive, keep personal and work accounts separate.

Spotting Fake Accounts and Phishing

RED FLAGS 	ACTION 
- Accounts with no photo, very few followers, or newly created. - Messages promising prizes or warning of account suspension - People pretending to be someone you know - Suspicious links sent through messages	BLOCK AND REPORT fake accounts. CONFIRM message directly with the person through a trusted channel. CHECK suspicious links before opening them. DO NOT click unknown links.

IF YOU THINK YOUR ACCOUNT HAS BEEN HACKED



Act fast.
Secure your
account.
Protect your
identity.



Quick action can stop damage
and help you regain control.



01

CHANGE YOUR PASSWORD IMMEDIATELY.

Create a strong, unique password you haven't used before.



02

LOG OUT OF ALL DEVICES.

Sign out of your account on all devices, especially those you don't recognize.



03

TURN ON EXTRA SECURITY (2FA) IF NOT ALREADY ACTIVE.

Two-Factor Authentication adds a strong extra layer of protection.



04

CHECK AND REMOVE UNKNOWN APPS CONNECTED TO YOUR ACCOUNT.

Review your account's connected apps and remove anything suspicious.



05

NOTIFY TRUSTED CONTACTS THAT YOUR ACCOUNT MAY BE COMPROMISED AND ALSO CONTACT YOUR MOBILE SERVICE PROVIDER IMMEDIATELY to report the issue and request SIM replacement protection if needed.



STAY ALERT. STAY SECURE.

Your security. Your responsibility.



Be aware today.
Stay safe tomorrow.

3.3 Understanding Data Privacy on Social Media

Social media apps and accounts don't just show your posts, they also collect information about you. Knowing what is collected and how to control it helps you stay safer online.

What information is collected?

- Personal details (name, phone number, email)
- Location data (where you are or have been)
- Contacts and connections
- Your activity (likes, shares, searches, messages)

Who can access it?

- The platform itself, Advertisers and third parties.
- Sometimes other users, depending on your settings.

How to protect your privacy

- Check your privacy settings: Control who can see your posts and profile
- Limit what you share: Avoid posting sensitive details (location, ID, travel plans)
- Turn off location sharing when not needed
- Review app permissions: Only allow access that is necessary
- Think before posting about others: Get consent before sharing their photos or information

Key Message: *Use social media wisely—protect your privacy, share carefully, and stay alert to risks.*

MODULE 4

STAYING SAFE FROM ONLINE HARM HARASSMENT, DOXXING AND SURVEILLANCE.

Women Human Rights Defenders (WHRDs) and women leaders who speak publicly, especially those advocating on gender, politics, land rights, or justice, face disproportionate online violence. These attacks can be stressful and harmful, but there are ways to protect yourself and respond safely. This module will help you understand these threats and how to defend yourself against them.

4.1 Online Harassment

This is repeated or severe abusive behavior carried out on digital platforms, including insults, threats, degrading comments intended to intimidate or silence someone, unwanted messages, impersonation, coordinated harassment and sustained campaigns of abuse designed to silence women's voices.

Prevention Strategies

- Check your social media profiles regularly and remove personal details like your home address, phone number or family information.
- Use a separate email for public or advocacy work that does not reveal your identity.
- Limit who can comment or reply to your posts, especially during sensitive high-visibility campaigns.
- Pre-plan a support network: identify who you will contact if you face online harassment.

If Harassment Occurs

- Take screenshots of everything such as messages, usernames, dates, and links (include URLs and timestamps).
- Do not respond to harassers, as such engagement can escalate attacks.
- Use platform tools to block, mute and report the accounts.
- Tell trusted colleagues or your support network immediately.
- Consider taking a short break from social media or making your accounts private, and respond by using appropriate mitigation measures such as issuing a clarification statement if necessary, seeking support from trusted networks and accessing mental health or psychosocial support if the situation affects your wellbeing.

If You Receive A Threat of Physical Violence

- Take all threats seriously.
- Screenshot and securely preserve all evidence immediately.
- Report to police and document and get an OB number.
- Alert your organization's security focal point or a trusted support person.
- Consider temporarily avoiding predictable routines and locations for your safety.

4.2 Doxxing

This means publishing someone's private personal information (home address, phone number, family details) online without consent to expose or incite harassment against them.

How to Protect Yourself

- Regularly search your name and phone number online to see what is publicly available about you.
- Use a Postal Address (P.O.BOX) or your organization's address for any public registrations.
- Keep your family members' information off your public profiles.
- Consider using a pseudonym (different name) for sensitive work if your safety requires it.

4.3 Digital Surveillance

Digital surveillance is when someone monitors your phone, messages, location, or online activity without your knowledge. This can be done by state actors, individuals, intimate partners, employers or even criminal networks. It may involve monitoring communications, tracking location or installing spyware on your device.

Emergency Contacts

Kenya-based support (legal, GBV & digital rights):

ORGANIZATION	SERVICE
<i>Centre for Rights Education and Awareness (CREAW)</i>	Provides psychosocial support, legal aid, and response services for survivors of gender-based violence, including technology-facilitated GBV such as online harassment and image-based abuse.
<i>Federation of Women Lawyers in Kenya (FIDA-Kenya)</i>	Offers legal aid, counselling, and justice support for women experiencing GBV, including online abuse, cyberstalking and digital harassment.
<i>Kenya ICT Action Network (KICTANet)</i>	Works on digital rights advocacy, internet governance, and digital safety awareness, including issues affecting online safety in Kenya.

<i>Article 19 Eastern Africa</i>	Defends freedom of expression and access to information, including support on digital rights, online safety, and protection of civic space in Kenya and the region.
----------------------------------	---

Digital security (Global support):

<i>Access Now</i>	24/7 Digital Security Helpline offering free support for hacking, account takeovers, surveillance, and online threats in multiple languages.
<i>Front Line Defenders</i>	Provides digital and physical security support for human rights defenders, including risk assessments and emergency protection guidance.
<i>Electronic Frontier Foundation</i>	Offers guides, tools, and legal resources to help people protect privacy, security, and digital rights online.

Key Message: *Online threats are real, but you are not alone. By staying alert, protecting your information, and seeking support early, you can reduce risk and stay safer online.*

MODULE 5

SECURE COMMUNICATION AND TOOLS

The tools you use to talk and share information online affect how private and safe your conversations are. Some apps protect your information better than others.

5.1 Messaging Apps: What You Should Know

TOOL	PRIVACY LEVEL	KEY NOTES
Signal	Highest — Recommended	End-to-end encrypted by default for all messages and calls. Open source, no ads, no data collection. Enable disappearing messages for sensitive conversations.
WhatsApp	Good	End-to-end encrypted messages but owned by Meta. Metadata (who you talk to, when, how long) is collected. Use for everyday communication; prefer Signal for sensitive discussions.
Telegram	Caution	Regular chats are NOT end-to-end encrypted. Only 'Secret Chats' offer E2EE. Many group chats are not encrypted. Use with caution for sensitive discussions.
SMS/Text Message	Not Secure	Not encrypted. Can be intercepted by mobile carriers and law enforcement. Avoid it for sensitive communications entirely.
Regular phone calls	Not Secure	Not encrypted. Can be intercepted. Use Signal calls for sensitive voice conversations.
Standard email (e.g. Gmail, Outlook)	Not Encrypted	Convenient but less private, so avoid for sensitive work. Use ProtonMail for sensitive email communications. End-to-end encrypted email. Free tier available. Based in Switzerland. Messages to other ProtonMail users are automatically encrypted. Tutanota – Secure email option with good privacy features. End-to-end encrypted email with calendar. Free tier available. Open source.

5.2 Getting Started with Signal

If you want to use a safer messaging app, Signal is a good option.

- Download Signal **only from** trusted app stores.
- Register using your phone number.
- Set a security PIN to protect your account.
- **Turn on** disappearing messages for sensitive chats.
- Add a screen lock inside the app.
- **Confirm** you are talking to the right person when possible.

5.3 Using a Virtual Private Network (Extra Internet Protection)

VPN is a service that encrypts your internet traffic and hides your IP address, protecting your browsing from surveillance on public networks. A VPN helps protect your internet use, especially on public Wi-Fi.

- It helps hide what you are doing online.
- It protects your information when using public Wi-Fi (like in cafes or airports).
- Avoid free VPNs because they may not be safe.
- Use trusted options like Proton VPN – Free option. Strong privacy protection (no ads or data selling). Best for safe browsing, email, messaging and public Wi-Fi protection. NordVPN Paid option. High-level security and strong encryption, Large global server network for safer digital access. Best for WHRDs needing consistent, high-security protection across all devices.
- A VPN adds protection, but it does not make you completely invisible online.

5.4 Secure Ways To Store And Share Files Online

ProtonDrive	End-to-end encrypted cloud storage. Good for sensitive documents. Free tier available.
OnionShare	Share files anonymously over the network. No account needed.
Dropbox	Convenient but NOT end-to-end encrypted. Avoid it for highly sensitive files.

Key Message : Choose your communication tools carefully. For private or sensitive work, always use secure apps that protect your messages and data.

MODULE 6

LEGAL FRAMEWORKS AND REPORTING MECHANISMS IN KENYA

Knowing and understanding your legal rights is as important as knowing your technical tools. Kenya has a growing legal framework protecting digital rights, although implementation remains a challenge. This module will help you understand the laws in Kenya.

- **Constitution of Kenya, 2010** - Article 31 (Right to Privacy), Article 33 (Freedom of Expression), Article 34 (Freedom of Media), Articles 49-51 (Rights of Arrested Persons).
- **Computer Misuse & Cybercrimes Act, 2018** - Criminalizes unauthorized access, identity theft, computer fraud, cyberbullying and publication of false information. Can be used to REPORT crimes against you but has also been used AGAINST activists. Know both dimensions of this law.
- **Data Protection Act, 2019** - Gives you rights over your personal data. You can request deletion of your data. The Office of the Data Protection Commissioner (ODPC) enforces this Act.
- **Sexual Offences Act, 2006** - Addresses sexual harm connected to digital abuse but TFGBV cases are mainly handled under Kenya's cybercrime and data protection laws especially when abuse happens online.
- **Penal Code** - Sections covering threatening communications and criminal defamation may apply to some online harassment cases.

6.1 How and Where to Report

Body	Mandate	Contact
DCI Cybercrime Unit	Kenya's primary cybercrime law enforcement body.	Toll-free: 0800722203 Email: cybercrime@dc.go.ke
Communications Authority of Kenya (CAK)	Regulates online content; can act on harmful content hosted on Kenyan platforms.	Website: https://www.ca.go.ke/
Office of the Data Protection Commissioner (ODPC)	Lodge complaints about misuse of your personal data.	Website: https://www.odpc.go.ke/
Article 19 Eastern Africa	Digital rights advocacy and legal advice on freedom of expression cases.	Website: https://www.article19.org/ Phone: +254 20 386 1536

Center for Rights Education and Awareness (CREAW)	Provides legal aid, psychosocial support, and advocacy for women and girls experiencing gender-based violence including TFGBV	Toll free line: 0800 720 186 Email: info@creaw.org / safeguarding@creawkenya.org Website: https://home.creaw.org/
Defenders Coalition	Supports the safety, security, and wellbeing of human rights defenders in Kenya.	+254 716 200 100 / +254 712 632 390 Toll-free emergency line: 0800 722 292 Email: info@defenderscoalition.org Website: https://defenderscoalition.org/
National Police Service	File a report and request an OB number for threats involving physical safety risk.	Call: 999 or visit nearest police station.
Coalition on Violence Against Women (COVAW)	Support for technology-facilitated gender-based violence.	Website: https://covaw.or.ke/ GBV Toll Free Line: 0800 720 553 Office: +254 722 178 177
Kenya Human Rights Commission (KHRC)	Legal support for WHRDs.	Website: https://khrc.or.ke/ Phone: +254 20 387 4998
National Council for Persons with Disabilities (NCPWD)	Disability rights complaints including inaccessible digital services.	Website: https://ncpwd.go.ke/ Toll Free Line: 0800 724 333 Phone: 020 2375994/ 020 2314621/ 0709 107 000
Wangu Kanja Foundation	Supports survivors of sexual and gender-based violence through medical, psychosocial, legal, and justice support.	+254 722 790 404 / +254 774 746 699 Toll free line: 1519 Email: info@wangukanjafoundation.org Website: https://wangukanjafoundation.org/

6.2 Documenting Incidents for Legal Purposes

- Preserve evidence immediately i.e. screenshot all abusive messages, posts, or threats with timestamps.
- Record URLs, usernames, profile links and timestamps for all evidence.
- Keep a written log: date, time, what happened, your response and witness names.
- Store copies in a secure location not only on a single device.
- Seek legal advice before engaging publicly with perpetrators.

Know Your Rights If Contacted by Police

- You have the right to remain silent and to legal representation (Article 50, Constitution of Kenya, 2010).
- The Computer Misuse & Cybercrimes Act has been used to target activists and journalists. If you are contacted by police regarding your online activity, seek legal advice immediately before cooperating.
- Contact KHRC or Article 19 immediately if you face legal pressure related to your digital activism.

Key Message: *Know your rights, understand the law and use available reporting mechanisms to protect yourself and seek justice online.*

MODULE 7

BUILDING A SAFE DIGITAL PRESENCE AND ADVOCACY

Safety does not mean silence. This module helps you build a confident, strategic digital presence that amplifies your advocacy work while managing your risks thoughtfully

7.1 Strategic Identity Management

Strategy	When To Use It
Full public identity	When your public visibility is itself a protection strategy and your work benefits from your real name and face being known.
Professional persona (real name, curated information)	When you want to be findable for professional opportunities but limit personal details publicly.
Pseudonym / Partial Identity	When your advocacy work exposes you to threats or when you need to protect sources, colleagues or community members.
Anonymous accounts	For the most sensitive work investigating abuses, supporting survivors or operating in high-risk environments.

7.2 Effective and Safe Digital Advocacy

Digital platforms offer Women Human Rights Defenders (WHRDs) powerful tools to amplify their voices and drive change. However, effective advocacy requires balancing visibility with safety by using clear messaging, choosing appropriate platforms, and engaging audiences responsibly. WHRDs should protect personal and sensitive information, use privacy and security tools, and

be mindful of risks such as harassment, misinformation and coordinated attacks. Building trusted support networks and planning for potential risks helps ensure that advocacy efforts remain both impactful and secure.

Building Audience and Visibility Safely

- Choose primary platforms based on where your audience is but do not rely on a single platform. Platforms can suspend accounts or shut down.
- Consider a website or blog as a stable home for your work that cannot be taken down by a platform's policy changes.

Content Strategy for High-Risk Advocacy

- Think about timing: posting about an ongoing situation in real-time can expose your location or compromise an operation.
- Prepare a crisis communications plan: what will you do if your accounts are suspended, hacked, or if you face a coordinated harassment campaign?
- Identify a trusted colleague who can post on your behalf or alert your community if you need to go offline unexpectedly.

Coalition and Solidarity

- Join networks of WHRDs and allies for mutual support.
- Document and amplify attacks on other WHRDs. Solidarity increases visibility and accountability.
- Set up a buddy system: a trusted person who checks in on you and can raise alarm if you become unreachable.

7.3 Self-Care and Digital Wellbeing

Sustained exposure to online harassment and threats takes a serious mental and emotional toll. Protecting your wellbeing is not a luxury, it is necessary for the sustainability of your work.

What to do

- Set boundaries on media consumption by designating offline hours, especially before sleep.
- Designate trusted colleagues to monitor mentions and flag urgent content so you do not have to be online constantly.
- Document harassment for evidence purposes, but do not read or re-read abusive content more than necessary.
- Seek professional mental health support. Befrienders Kenya: 0800 723 253 (toll-free).
- Know that online violence is not your fault and you are not alone.

Building a Resilient Digital Strategy

- Back up your content regularly to an external drive and secure cloud storage.
- Have a written crisis plan: who to call, what to do, who takes over if you need to step back.
- Train at least one trusted colleague in these same digital safety practices.
- Review and update your threat model every six months or after a major life or work change.

Key Message: *Solidarity is itself a security strategy build and invest in your support networks.*

MODULE 8:

DISABILITY INCLUSION IN DIGITAL SPACES

This module ensures that all women, including women with disabilities, can safely use digital tools and participate online. It is for women with disabilities and for everyone who works alongside them.

Why does this matter?

- Women with disabilities face higher risks of online abuse and exclusion.
- Many digital platforms are not designed to be accessible.
- Barriers like cost of assistive tools, inaccessible apps, and stigma make it harder to participate.
- Inclusion is a legal right under the Constitution of Kenya, 2010 and disability laws.

8.1 Common Challenges and Practical Solutions by Disability Type

For women with visual impairment

Challenges	Solutions:
Images without descriptions, difficult security steps	• Turn on screen readers (TalkBack or VoiceOver) • Use apps that work well with screen readers (e.g. password managers) • Use app-based verification instead of phone calls • Increase font size and display settings to make text easier to read on your device

For women with physical disabilities

Challenges	Solutions:
Difficulty typing or navigating devices	• Use voice commands or assistive touch features • Set quick screen lock options for safety • Limit who can access your device

Challenges	Solutions:
Complex instructions, higher exposure to scams or distress. Flashing images or videos can cause discomfort, stress, or seizures.	• Use simple passwords that are easy to remember but safe. • Take time before responding to urgent or scary messages. • Reach out to someone you trust when unsure. • Avoid content with flashing or rapidly blinking lights. • Turn on accessibility settings that reduce motion or flashing effects. • Use apps and devices in dark mode or low-brightness settings. • Take breaks from screens when feeling overwhelmed or uncomfortable.

8.2 How to make digital spaces more inclusive

8.2 HOW TO MAKE DIGITAL SPACES MORE INCLUSIVE

Small changes make a big difference. Inclusive content makes the digital world **work for everyone**.



1 USE SIMPLE AND CLEAR LANGUAGE (ONE IDEA AT A TIME)



- ✓ Short sentences.
- ✓ Active voice.
- ✓ One idea at a time.

Clear language is easy to read and easy to understand.

2 ADD DESCRIPTIONS TO IMAGES (WHO, WHAT, WHERE)

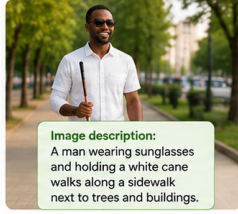
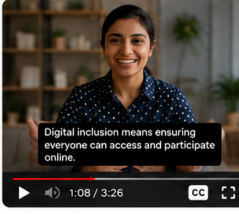


Image description:
A man wearing sunglasses and holding a white cane walks along a sidewalk next to trees and buildings.

Descriptions help everyone understand the full picture.

3 ADD CAPTIONS TO VIDEOS AND CHECK THEY ARE CORRECT



Digital inclusion means ensuring everyone can access and participate online.

Captions help people who are deaf or hard of hearing — and everyone, everywhere.

4 USE CLEAR FONTS AND AVOID FLASHING OR CONFUSING DESIGNS

Aa

Clear font. Good contrast.

FLASH!

Avoid flashing, clutter and low contrast.

Clear design helps everyone focus and feel comfortable.

5 SHARE INFORMATION IN DIFFERENT FORMATS (TEXT, AUDIO, VIDEO)

Text

Easy to read and refer to.

Audio

Listen on the go.

Video

See it in action.

Different formats reach more people in more ways.

8.3 Respect and Safety for Women with Disabilities Online

- Do not share someone's disability or health information without their permission. Under the Data Protection Act 2019, disability data is sensitive and legally protected.
- Use respectful language (e.g. "woman with disability"), 'psychosocial disability' not 'mentally ill'. Avoid harmful or offensive terms
- Support people facing discrimination online. Report ableist content on platforms. Amplify content created by women with disabilities.
- Ask before helping , do not assume. Proactively ask about access needs at all events.
- Always speak directly to the person with a disability, not only to their aide, interpreter or caregiver when they are present.

8.4 Quick Checklist Before You Post Online

- The language is simple and clear — jargon explained, short sentences, no ALL CAPS.
- Every image has an alt-text description.
- Every video has captions or subtitles.
- I have not disclosed anyone's disability or health status without their consent.
- I have used respectful, person-first language where disability is mentioned.
- The content is shared in more than one format where possible.

Key Message : *Digital spaces must include everyone, making content accessible is not optional but a legal right, and Women With Disabilities should always be actively involved in shaping the solutions that affect them.*



Community Advocacy & Awareness (CRAWN) Trust
4th Floor All African Conference of Churches of Kenya, Waiyaki Way, Westlands.
P.O Box 943-00621, Nairobi, Tel: 020-2664505, E-mail: crawn@crawntrust.org

© CRAWN Trust