

FOR WOMEN IN NIGERIAN POLITICS,
CIVIL SOCIETY, AND PUBLIC LIFE

Digital Safety Toolkit

A practical defence guide for
the 2027 election cycle and beyond



SUPPORTED BY:



Digital Democracy
Initiative



FOR WOMEN IN NIGERIAN POLITICS,
CIVIL SOCIETY, AND PUBLIC LIFE

Digital Safety Toolkit

A practical defence guide for
the 2027 election cycle and beyond

Covering secure account management, VPN use, harassment
reporting, and documentation of gendered disinformation

SUPPORTED BY



Digital Democracy
Initiative

First Edition | September 2026

How to use this toolkit

This is a working reference, not a book to be read cover-to-cover. It is designed to sit on your phone or your desktop and be consulted when you need it. The six sections each stand alone:

- **Section 1 — Understanding the threat landscape:** the conceptual foundation. Read once. Comes back to mind under attack.
- **Section 2 — Secure account management:** the work-through-it-once-and-be-done-with-it section. Do it on a calm day, not in a crisis.
- **Section 3 — VPN and network hygiene:** what a VPN actually does, when it helps, when it does not. Reference as needed.
- **Section 4 — Online harassment reporting procedures:** the protocols. Read in advance; reference when you need to act.
- **Section 5 — Documentation strategies:** how to capture and preserve evidence of attacks against you. Templates included.
- **Section 6 — Pre-campaign safety plan:** the consolidated 30-day plan and the 24-hour incident playbook.

Four annexes follow: a glossary, printable quick-reference cards, a Nigerian resource directory, and reporting templates. The toolkit is designed so that you can print Section 6 and the annexes for offline use; everything else assumes you are reading on a connected device.

A note on safety planning

There is no single “secure” configuration that works for everyone. Your safety plan depends on what you do, where you do it, and who you are. The recommendations in this toolkit are general-purpose defaults that will materially improve the safety of almost every woman in Nigerian politics. They are not personalised security advice. If you are in immediate danger, or if you are a high-profile target, please contact one of the organisations listed in Annex C — most of them can provide individualised support and will respond confidentially within 24 to 72 hours.

Who this toolkit is for

This toolkit is for any woman whose participation in Nigerian public life puts her in a position to be targeted by online attacks. That includes, but is not limited to:

- Women political aspirants and candidates at federal, state, and local-government level;
- Women party officials and political appointees;
- Women activists, advocates, and civil society leaders;
- Women journalists covering politics, security, or gender;
- Women academics, researchers, and commentators on Nigerian politics;
- Members of women-led coalitions, NAWOJ chapters, FIDA chapters, and JONAPWD chapters with public-facing work;
- Anyone else whose political visibility creates exposure to gendered attack.

The toolkit is also useful — and free to share — with anyone supporting women in these positions: campaign managers, family members, communications officers, and allies.

What this toolkit is not

This toolkit cannot do certain things, and we want to be honest about that up front.

- **It cannot make you anonymous.** Most women in Nigerian politics need to be visible — that is the point. The goal here is to manage visibility, not eliminate it.
- **It cannot stop motivated state actors.** If a national security agency wants to monitor you, no consumer-grade defence stops them. The threats this toolkit defends against are the ones that affect almost everyone: criminal opportunism, partisan harassment, and the industrialised disinformation infrastructure documented in Nigerian elections.
- **It cannot replace legal advice.** Where the toolkit references Nigerian law (the NDPA, the Cybercrime Act, the Violence Against Persons Prohibition Act), it does so for orientation. Specific legal questions need a lawyer; the resource directory in Annex C points to women's legal-aid organisations.
- **It cannot keep pace with every platform change.** Platforms reshuffle their settings menus frequently. The principles in this toolkit are durable; the click-paths in the platform-specific sections may have shifted slightly by the time you read them. The principle is reliable; the precise menu name might not be.

Contents

Section 1. Understanding the Threat Landscape	5
1.1 Online gender-based violence (OGBV)	5
1.2 Gendered disinformation	5
1.3 Doxxing and coordinated identification	6
1.4 The Liar's Dividend and women's testimony	6
1.5 Why Nigerian women in politics face heightened risks	7
Section 2. Secure Account Management	8
2.1 Strong passwords and password managers	8
2.2 Two-factor authentication	9
2.3 Platform-by-platform hardening	10
2.4 Account recovery and backup	12
2.5 Device security basics	12
Section 3. VPN and Network Hygiene	14
3.1 What a VPN does, and does not	14
3.2 When to use a VPN	14
3.3 Choosing a VPN	15
3.4 Public Wi-Fi safety	15
3.5 Encrypted messaging and Signal	16
Section 4. Online Harassment Reporting Procedures	17
4.1 First response: document before you act	17
4.2 Platform reporting	18
4.3 Nigeria Police Force and law enforcement	19
4.4 Civil society and legal aid pathways	20
4.5 Psychosocial support	20
4.6 When to involve trusted media	21
Section 5. Documentation Strategies for Gendered Disinformation	22
5.1 Why documentation matters	22
5.2 The capture-and-archive method	22
5.3 Timestamping and chain of custody	23
5.4 Metadata preservation	24
5.5 What goes into a documentation file	25
5.6 Coordinating with fact-checkers	25
Section 6. Pre-Campaign Safety Plan	26
6.1 The 30-day pre-campaign checklist	26
6.2 The 24-hour incident response playbook	27
6.3 Building your circle of support	28
Annex A — Glossary	30
Annex B — Quick-reference cards (printable)	32
Annex C — Nigerian resource directory	33
Annex D — Reporting templates	35

1

Understanding the Threat Landscape

Before reaching for tools, be clear about what those tools are defending against. Four distinct categories of attack — because the defences against each are different.

Most women in Nigerian politics describe “online abuse” or “trolling” as a single phenomenon. It is more useful to break it into four distinct categories — because the defences against each are different.

1.1 Online gender-based violence (OGBV)

Online gender-based violence is the spectrum of harms enabled by digital technologies that target a person because they are a woman. The defining characteristic is that the attack is gendered — it draws on the target’s status as a woman to produce harm — rather than incidental.

The most common forms of OGBV that women in Nigerian politics face include:

- **Direct harassment and threats:** messages containing insults, slurs, or threats of physical or sexual violence, typically delivered via DMs, replies, or mentions.
- **Sexualised content:** messages, comments, or images framing the target in sexual terms — explicit propositions, lewd commentary, fabricated sexual histories.
- **Non-consensual intimate image distribution:** publication of intimate photographs or videos without the subject’s consent. This includes both authentic images obtained without consent and fabricated images, including AI-generated synthetic content.
- **Stalking and surveillance:** persistent unwanted contact across multiple accounts and platforms, sometimes accompanied by attempts to map the target’s movements.
- **Impersonation:** creation of fake accounts using the target’s name and likeness, often to post damaging or compromising content as if it were her.

OGBV is often dismissed by observers as “just words on the internet,” particularly by people who do not experience it. The empirical record is clear: women political aspirants and activists in Nigeria consistently identify OGBV as among the most consequential reasons they consider leaving public political life. The cumulative effect on the broader pool of women considering politics is to depress recruitment.

1.2 Gendered disinformation

Gendered disinformation is a specific subset of disinformation in which false information is deployed against a woman, drawing on gender stereotypes to undermine her credibility, fitness for office, or claim to public voice.

The Brain Builders Youth Development Initiative (BBYDI) catalogues this as encompassing “sexualised content, sexist and misogynistic content, and the posting of doctored images and videos aimed at ridiculing women based on their gender.” In the Nigerian 2023 cycle, gendered disinformation took several recognisable forms:

- **Marital-status shaming:** fabricated stories about divorce, infidelity, or alleged sexual histories used to position the target as morally unfit for office.
- **Body-shaming and appearance manipulation:** doctored or AI-generated images altering the target's appearance for ridicule.
- **Religious or ethnic disloyalty narratives:** fabricated claims that the target has betrayed her religious or ethnic community, often coupled with imagery designed to provoke specific community responses.
- **Family-instability framings:** stories suggesting the target neglects her children or household responsibilities — a charge essentially never made against male politicians.
- **Misidentification campaigns:** the Oyefusi pattern — a photograph of a different woman in a compromising situation is falsely attributed to the target.

Unlike OGBV, which targets individuals, gendered disinformation operates on the broader narrative environment. It produces stories that take on a life of their own — circulating beyond the original target, shaping the way voters think about female candidates in general, and entering political discourse as if it were ordinary news. The Wilson Center's 2020 "Monetizing Misogyny" study documented false claims about then-Vice-Presidential candidate Kamala Harris being shared at peaks of 3,000 times per hour on Twitter — a volume only achievable with coordinated, semi-automated production. The Nigerian 2027 cycle should be expected to see comparable volumes against high-profile female aspirants.

1.3 Doxxing and coordinated identification

Doxxing — the public release of private information about a person, particularly their home address, family details, financial information, or personal contacts — has become a standard tactic in attacks on Nigerian women in politics. The information may be:

- Genuine, compiled from public records and social media archaeology of family members;
- Fabricated, constructed by hostile actors to appear plausible;
- Mixed, with some authentic information surrounded by fabrications to give the package credibility.

In Nigeria's current security environment, doxxing is materially dangerous. A woman whose home address is published alongside accusations of religious or ethnic disloyalty in regions with active intercommunal tensions is at heightened physical risk. A woman whose family members' details are published may be the conduit through which threats arrive at people who did not choose public political life.

Defending against doxxing means assuming, from the outset, that information you make available now will be aggregated against you later. The Pre-Campaign Safety Plan in Section 6 includes specific steps to reduce your doxxing surface.

1.4 The Liar's Dividend and women's testimony

The most insidious effect of generative AI on women in politics is not the deepfakes themselves but the doubt their existence sows about all media — including women's own accounts of what is being done to them.

Once "AI-generated content" becomes a known category that voters are aware of, every authentic piece of evidence inherits the suspicion attached to its synthetic counterpart. When a woman in Nigerian politics produces evidence of an attack against her — screenshots, recordings, witness accounts — the response is increasingly "how do we know this is real?" The category does the corrosive work; no specific deepfake is required.

Hannah Ajakaiye of FactsMatterNG has documented Nigerian cases of this dynamic, including political figures dismissing authentic damaging recordings as "AI-manipulated." Women are particularly vulnerable to this dynamic

because, in the prevailing narrative environment, women's testimony is already treated as more contestable than men's. The Liar's Dividend amplifies an existing bias.

Section 5 of this toolkit covers documentation strategies specifically designed to preserve the integrity of your own testimony — so that the evidence of what is being done to you cannot be quietly contested into nothing.

1.5 Why Nigerian women in politics face heightened risks

Four structural features of the Nigerian information environment make the threat landscape for women in politics particularly acute:

1. **Indigenous-language attacks are essentially unmoderated.** Production-side AI can now produce fluent Hausa, Yoruba, Igbo, and Pidgin content. Detection-side AI on the platforms cannot. A woman whose name circulates in any indigenous language is operating in a space where content moderation does not effectively reach.
2. **WhatsApp is the dominant channel for sustained attacks against women, and it is opaque.** The encrypted, closed-group architecture means that fact-checkers, platforms, and even the women themselves often cannot see the attacks circulating in WhatsApp groups.
3. **The 2023 election demonstrated that the paid-influencer infrastructure is industrialised.** The same coordination machinery that targets opposing candidates can be — and is — turned against women specifically. Coordinated campaigns against female aspirants can produce hundreds of near-identical posts within minutes.
4. **Institutional response infrastructure remains nascent.** INEC's AI Division was only established in May 2025. No election-specific synthetic-media law is yet in force. The 2027 cycle will be contested under a legal regime designed before AI-enabled attacks were a credible threat.

None of this is intended to discourage you from public political life. Quite the opposite. The point of this toolkit is to give you the practical tools to do that work safely — because the alternative, in which women cede public political life to those willing to operate without these defences, is intolerable.

2

Secure Account Management

Account hardening is mostly free, mostly fast, and mostly permanent. Once configured properly, accounts stay hardened — the heavy lifting is one-time work.

Account compromise is the most common pathway through which serious attacks against women in politics escalate. An attacker who controls your email address controls every other account that uses that email for recovery. An attacker who controls one social-media account can post on your behalf, harvest your DMs, and use the captured account to attack other women in your network. The work in this section is therefore the foundation on which everything else sits.

The good news: account hardening is mostly free, mostly fast, and mostly permanent. Once configured properly, accounts stay hardened. You will need to revisit settings every six to twelve months, but the heavy lifting is one-time work.

2.1 Strong passwords and password managers

The two rules of password security are:

1. **Every account gets its own password.** Re-using passwords across accounts is the single most common cause of account compromise. When one platform suffers a breach (and platforms suffer breaches constantly), every account where you used the same password is exposed.
2. **Passwords should be long, random, and unmemorable.** The strongest password is one you cannot remember — generated by a password manager and stored there. Sixteen characters minimum; twenty or more for critical accounts.

The only practical way to follow these rules is a password manager. A password manager is a small piece of software that generates unique, strong passwords for every site you use and remembers them for you. You memorise one strong master password; the manager handles the rest.

Recommended password managers

TOOL	COST	NOTES
Bitwarden	Free (paid tier available)	Open source, audited, works on every major platform. The recommended default for most users. Free tier is genuinely usable.
1Password	Paid (~\$36/year)	Polished interface, excellent for families and teams. The best choice if you can afford it.
KeePassXC	Free	Offline-only, stores your password database locally. Most paranoid option; requires more setup.

Your master password

Your password manager protects you with one password — the master password. This is the only password you ever need to memorise. It must be strong and unique. Two reliable approaches:

- **The four-word phrase method:** choose four random, unrelated words and a number — for example, 'kettle-mango-pyramid-violin-7'. Long enough to resist brute-force, easy enough to remember. Do not use words from your personal life; use random ones.
- **The full sentence method:** a memorable phrase that no one knows, with deliberate alterations — for example, the first line of a song you love, with deliberate substitutions you can recall. 16+ characters.

Never write your master password down on a device. If you must write it down at all, do it on paper, store it in a physically secure location (a safe at home, for example), and treat it like cash.

2.2 Two-factor authentication

Two-factor authentication (2FA) means that logging in requires both something you know (your password) and something you have (a code from an app on your phone, or a hardware key). Even if an attacker steals your password — through a data breach, a phishing email, or a stolen device — they cannot access your account without the second factor.

2FA is the single highest-return security control available to you. Of every defensive measure in this toolkit, 2FA is the one that most cleanly closes the most attack vectors.

The three types of 2FA, ranked

METHOD	STRENGTH	WHEN TO USE
Hardware key (YubiKey, Google Titan)	Highest	On every account that matters, if you can afford it. Phishing-resistant in a way nothing else is. Cost: ₦15,000–₦30,000 per key; buy two so you always have a backup.
Authenticator app (Authy, Google Authenticator, Microsoft Authenticator)	Strong	The default for every account. Free, takes two minutes to set up per account. Authy is recommended because it supports encrypted backup to a second device.
SMS code (text message)	Weakest	Better than no 2FA at all. But SIM-swap attacks are documented in Nigeria; if SMS is your only 2FA, an attacker who captures your number controls your accounts.

On SIM-swap attacks

A SIM swap happens when an attacker convinces your mobile operator to transfer your phone number to a SIM card they control. Methods range from social engineering (calling customer service and impersonating you) to insider corruption (paying an employee at the network). Once they have your number, they receive your SMS codes and intercept your calls. Defences: ask your operator to put a PIN or port-protection on your account; do not use SMS as your primary 2FA for any account that matters; and consider keeping a separate, unpublicised SIM for account-recovery purposes only.

Order of operations for 2FA setup

Turn on 2FA in this order, because the order matters. Your email account is the master key — if it falls, everything else does.

1. Your primary email account (Gmail, Outlook, ProtonMail). This is the highest priority.
2. Your password manager itself (most password managers offer 2FA on the master account).
3. Every social media account: Facebook, X, Instagram, WhatsApp, TikTok, LinkedIn, YouTube.
4. Any cloud storage (Google Drive, Dropbox, OneDrive, iCloud).
5. Any payment or banking account that offers 2FA.
6. Government and identity portals where supported (some Nigerian government portals now offer 2FA).

Backup codes

When you turn on 2FA, every platform offers you a set of one-time “backup codes.” These are how you get back in if you lose your phone or hardware key. They are also a small but real risk if exposed. Recommended handling:

- Print backup codes to paper. Do not save them only on the device you log in from.
- Store the printed codes in a physically secure place — a safe, a locked drawer, or with a trusted person in a sealed envelope.
- Treat backup codes like cash. If they are lost, regenerate them through the platform and discard the old set.

2.3 Platform-by-platform hardening

Below are the specific settings to change on the platforms most commonly used in Nigerian political life. Platforms reshuffle their menus frequently; the click-paths below are accurate as of the publication of this toolkit but may require minor navigation if the platform has reorganised.

Facebook

- **Settings → Security and Login → Two-Factor Authentication** → set to “Authentication App.” Add Authy or Google Authenticator.
- **Settings → Security and Login → Where You’re Logged In:** log out of any session you do not recognise.
- **Settings → Security and Login → Get alerts about unrecognized logins:** turn ON for both email and notification.
- **Settings → Privacy** → review who can see your friends list, your posts, and your future posts. For a public-facing political account, set future posts to “Public”; for a personal account, set to “Friends.”
- **Settings → Profile and Tagging** → set “Who can tag you in posts” to “Friends”; set “Review tags before they appear on your profile” to ON.
- **Settings → Apps and Websites:** review every connected app. Remove anything you do not actively use.
- **Settings → Public Posts** → set “Who Can Follow Me” to “Public” only on your public account; on personal accounts, set to “Friends.”

X (Twitter)

- **Settings → Security and account access → Security → Two-factor authentication:** enable Authentication app. If you have a hardware key, add it too.
- **Settings → Security and account access → Apps and sessions:** review connected apps; revoke anything unfamiliar.

- **Settings → Privacy and safety → Direct Messages:** TURN OFF “Allow message requests from everyone.” TURN ON “Filter low-quality messages.”
- **Settings → Privacy and safety → Audience and tagging:** consider switching to Protected tweets for your personal account; leave your public account public.
- **Settings → Privacy and safety → Mute and block:** set up the muted-words feature with a list of slurs and harassment terms in the languages you operate in.
- **Settings → Notifications → Filters → Quality filter:** TURN ON. Also turn on “Mute notifications from” filters for accounts that are not following you, new accounts, and accounts with default profile photos.

Instagram

- **Settings → Security → Two-Factor Authentication:** Authentication App.
- **Settings → Privacy → Account Privacy:** for your personal account, set to Private. For your political account, leave Public but lock down the rest below.
- **Settings → Privacy → Messages:** set DMs to “People you follow” or “Your followers.” Restrict group invites to people you follow.
- **Settings → Privacy → Hidden Words:** turn ON “Hide Comments” and “Hide Message Requests” with both the default and your own custom-list filters.
- **Settings → Privacy → Comments:** turn ON “Manual Filter” with your custom-list filters.
- **Settings → Privacy → Tags and mentions:** set “Who can tag you” and “Who can @mention you” to “People you follow.”
- **Settings → Privacy → Story:** hide your story from harassers you cannot block (the account does not know it has been hidden).

WhatsApp

- **Settings → Account → Two-step verification:** TURN ON. Set a six-digit PIN. Provide a recovery email.
- **Settings → Privacy → Last seen and online:** set to “My contacts” or “Nobody.”
- **Settings → Privacy → Profile photo:** set to “My contacts.”
- **Settings → Privacy → About:** set to “My contacts.”
- **Settings → Privacy → Groups:** set to “My contacts.” This prevents strangers from adding you to groups.
- **Settings → Privacy → Disappearing messages:** consider turning on a 90-day default for sensitive conversations.
- **Settings → Privacy → Advanced → Protect IP address in calls:** TURN ON if available.

TikTok

- **Settings → Security → 2-step verification:** Authentication App.
- **Settings → Privacy → Direct messages:** set to “Friends” or “No one.”
- **Settings → Privacy → Comments:** filter all comments and review before they appear publicly.
- **Settings → Privacy → Comment filters:** add custom keywords in the languages you operate in.

Google account (the master account)

- **myaccount.google.com → Security → 2-Step Verification:** set up with Authenticator app AND, if available, a hardware key as backup.

- **myaccount.google.com → Security → Third-party apps with account access:** remove anything you do not currently use.
- **myaccount.google.com → Security → Your devices:** sign out of any device you no longer use.
- **myaccount.google.com → Security → Advanced Protection Program:** if you are a high-profile aspirant or political appointee, consider enrolling. APP imposes hardware-key-only sign-in and blocks third-party app access. It is strict; it is also the highest-security configuration Google offers.

2.4 Account recovery and backup

Recovery is the back door. Attackers know that if they cannot guess your password, they can still get in by manipulating the recovery flow. Strengthen recovery and you close a major vector.

Recovery email

Most platforms allow you to designate a recovery email — a backup address used if you cannot access your primary account. Two rules:

- **The recovery email must itself be hardened.** If your Gmail uses an old Yahoo account as recovery, and that Yahoo account has no 2FA, the chain is only as strong as the Yahoo account.
- **Use a dedicated recovery email.** Some users maintain a separate, never-publicly-used email address that exists only as a recovery contact. This address never receives normal mail; it cannot be guessed from your public profile.

Recovery phone

Where platforms still rely on SMS for account recovery, consider:

- Removing your phone number from recovery on critical accounts (where the platform allows).
- Using a separate “recovery SIM” — a number you do not publish, do not share, and use only for account recovery. Many Nigerian women in politics maintain a private SIM specifically for this purpose.
- Asking your mobile operator to put a port-protection PIN on your account. This is a free service most operators offer; few users know to ask for it.

Security questions

Where platforms still use “security questions” — “What was your mother’s maiden name?”, “What city were you born in?” — never answer truthfully. The truthful answers to these questions are findable on relatives’ social media and in public records. Use a long, random string and save it in your password manager.

2.5 Device security basics

All of the work above protects your accounts. The accounts live on devices, and devices need to be secured too. The principles are simple.

Your phone

- **Screen lock:** a six-digit PIN minimum; biometric (fingerprint or face) plus PIN is better. Avoid four-digit PINs; they fall to brute-force on a calm afternoon.
- **Operating system updates:** install them when prompted. Security updates close vulnerabilities that attackers actively exploit.
- **App permissions:** review which apps have access to your microphone, camera, location, and contacts. Revoke anything that does not need it.

- **Find my phone:** turn on Find My iPhone (iOS) or Find My Device (Android). If you lose the phone, you can locate or remotely wipe it.
- **Backups:** turn on automatic encrypted backup (iCloud for iOS; Google for Android). A lost phone with a clean backup is an inconvenience; a lost phone without a backup is a crisis.

Your laptop or desktop

- **Full-disk encryption:** turn on FileVault (Mac) or BitLocker (Windows Pro). If your laptop is stolen, the thief cannot read your files without your password.
- **Auto-screen-lock:** configure the screen to lock automatically after five minutes of inactivity.
- **Operating system updates:** install promptly. Same logic as phones.
- **Anti-malware:** on Windows, the built-in Defender is now adequate for most users; keep it on. On Mac, the built-in protections are sufficient. Add a layer (Malwarebytes Free) if you handle large volumes of email attachments or downloads.

The single highest-impact device decision

If you can afford it, separate your political work from your personal life at the device level. A dedicated political-work phone — different SIM, different accounts, different apps — limits the damage if either device is compromised. It also keeps personal photographs, family conversations, and unguarded moments outside the device that is exposed to your public role.

3

VPN and Network Hygiene

The network-level defences: VPN use, encrypted messaging, and what to do on public Wi-Fi — plus two pieces of common VPN advice worth correcting before they cause harm.

This section covers the network-level defences: VPN use, encrypted messaging, and what to do on public Wi-Fi. The principles here are simpler than the account-management section, but two pieces of common advice about VPNs are worth correcting before they cause harm.

3.1 What a VPN does, and does not

A Virtual Private Network (VPN) is a service that creates an encrypted connection between your device and a server operated by the VPN provider. Internet traffic from your device flows through that encrypted tunnel before it reaches its destination. Two practical consequences follow.

What a VPN actually does

- **It hides your real IP address** from the websites and services you visit. Those services see the IP address of the VPN server instead. This makes it harder for them to identify your physical location based on your IP.
- **It encrypts your traffic between your device and the VPN server.** On a public Wi-Fi network (a hotel, an airport, a café), this prevents someone on the same network from seeing the websites you visit and any unencrypted data you send.
- **It allows you to appear, to websites, as if you are browsing from a different country** — useful for accessing geo-blocked content.

What a VPN does NOT do

- **It does not make you anonymous to the VPN provider itself.** The VPN provider sees your traffic. The quality of a VPN's privacy promise depends entirely on whether the provider keeps logs and whether their no-logs policy has been audited.
- **It does not protect you against attacks targeting your accounts.** If your password is compromised, a VPN does not save you.
- **It does not protect against tracking by services where you are logged in.** If you are signed in to Facebook over a VPN, Facebook still knows it is you. The IP address change is irrelevant once you have authenticated.
- **It does not protect against deanonymisation by motivated state actors.** Consumer-grade VPNs defend against ordinary attackers, not against well-resourced surveillance operations.

3.2 When to use a VPN

Use a VPN in the following situations:

1. **Always on public Wi-Fi.** Hotels, airports, conferences, cafés. Public Wi-Fi networks are routinely surveilled by both casual snoopers and motivated attackers. A VPN closes that vector.

2. **When working in security-sensitive contexts.** If you are traveling, or operating in a region where you have reason to believe your traffic might be monitored, use a VPN.
3. **When accessing services that might track your IP for political reasons.** Some platforms log IP addresses for compliance purposes; if you would prefer that your home IP not be associated with sensitive research, a VPN helps.
4. **Routinely as a baseline, if your device is your main political-work tool.** Many security-conscious activists run a VPN by default.

3.3 Choosing a VPN

Three rules for choosing a VPN:

1. **Pay for it.** “Free” VPNs are not free; they typically monetise by collecting and selling your traffic data. The thing they are supposed to protect you from is the business model they operate on. Pay around USD 3 to 10 per month for a reputable service.
2. **Pick a provider with an independently audited no-logs policy.** The provider’s claim that they do not keep logs is worth nothing without third-party verification. Audited providers publish their audit reports.
3. **Pick a provider whose jurisdiction matches your threat model.** A VPN based in a country with strong privacy law and no compulsory data-retention obligation is safer than one based in a surveillance-friendly jurisdiction.

Recommended VPNs (June 2026)

PROVIDER	COST (APPROX.)	NOTES
Mullvad	€5/month flat	Sweden-based. Accepts cash and Monero (no identity required). Independently audited no-logs policy. The most privacy-respecting option.
Proton VPN	Free tier; paid ~\$10/mo	Swiss-based. From the makers of ProtonMail. Free tier is genuinely usable. Paid tier adds higher speeds, more locations, and Secure Core (multi-hop).
IVPN	~\$6/month	Gibraltar-based. Strong audit history. No-logs policy independently verified.

Avoid these red flags

Do not use a VPN that promises “lifetime” subscriptions for a one-time payment — these are usually fronts for data collection or are bought up and resold by data brokers. Do not use a VPN whose privacy policy you have not read. Do not use a VPN that has been the subject of public scandals about logging or data sharing. Do not use a VPN whose owners are unclear or change frequently.

3.4 Public Wi-Fi safety

Public Wi-Fi networks — hotels, airports, conferences, cafés, government buildings — are inherently low-trust. The network operator sees more of your traffic than you might expect; other users on the network can sometimes see what you are doing; and rogue Wi-Fi networks that imitate legitimate ones are a documented attack vector. Rules:

1. **Always use a VPN on public Wi-Fi.** Always.

2. **Do not connect to unknown networks.** “Free_Airport_WiFi” might be the airport’s; it might also be a rogue access point. Check the network name with airport staff before connecting.
3. **Turn off automatic Wi-Fi connection on your devices.** Otherwise your phone will silently connect to any network with a familiar name.
4. **Treat hotel Wi-Fi as you would treat a public café.** Hotel networks are not meaningfully more trustworthy than coffee-shop networks.
5. **If you are doing high-sensitivity work** — entering passwords, accessing financial information, communicating with sources — use mobile data through your phone’s hotspot instead of public Wi-Fi. Your cellular connection is materially more private than any public Wi-Fi.

3.5 Encrypted messaging and Signal

WhatsApp is the default messaging app for most Nigerians and is end-to-end encrypted, which is genuinely useful. But Meta — WhatsApp’s owner — does collect substantial metadata about who you message and when, even though message contents are encrypted. For most political conversations, WhatsApp is acceptable. For genuinely sensitive conversations — sources, legal counsel, security planning — there is a better option.

Signal (signal.org) is a free, open-source messenger that is widely regarded as the gold standard for encrypted communication. Unlike WhatsApp, Signal collects effectively no metadata. It is recommended by every major security organisation and is used by journalists, lawyers, and activists worldwide.

When to use Signal:

- Conversations with sources or whistle-blowers;
- Communication with your lawyer;
- Security planning and incident-response conversations;
- Any conversation you would not want metadata about — even just “who you spoke to and when” — accessible to a determined adversary.

Signal works on Android, iOS, and desktop. It is free. It does not show ads. It is funded by donations and a small foundation. There is no good reason not to install it.

4

Online Harassment Reporting Procedures

When an attack lands, the instinct is to react — and almost every instinct makes it worse. A tested response protocol used by women in politics, journalists, and activists globally.

When an attack lands, the instinct is to react — to respond, to delete, to engage. Almost every one of those instincts makes the situation worse. This section walks through a tested response protocol that has been used by women in politics, journalists, and activists globally. It applies whether the attack is a single threatening message, a coordinated harassment campaign, or a gendered disinformation operation.

The five-second rule

Before you do anything — before you reply, delete, screenshot, or call anyone — pause for five seconds and run through this checklist: Am I in physical danger right now? Is anyone I love in physical danger? Is this happening at multiple locations or just one? Have I documented anything yet? Five seconds. Then act.

4.1 First response: document before you act

The first rule of incident response is that you cannot defend what you have not documented. Before you block, report, or even read the rest of the harassment, capture the evidence. Section 5 of this toolkit covers documentation in depth; for incident-response purposes, the minimum capture is:

1. **Take screenshots of the harassment immediately.** Capture the post or message, the URL, the timestamp, the account that sent it, and any visible engagement metrics. If the harassment is a thread, capture the whole thread.
2. **If the content is in a video or audio format, screen-record it before it disappears.** Use your phone's built-in screen recorder. Capture audio if relevant.
3. **Save the URLs to a secure location** — your password manager's secure notes field, an encrypted folder, or a dedicated Signal note-to-self. URLs are how the platform's reporting tools find the content; lose the URL and reporting becomes much harder.
4. **Note the time you first saw the content.** Where possible, note the time the content was posted (visible on most platforms by hovering over the timestamp).
5. **Do not engage with the harasser.** Replying, even to refute, often amplifies the content algorithmically and gives the harasser the engagement they wanted. The single most effective response to most harassment in the first hour is silence-plus-documentation.

Once documentation is complete — typically five to fifteen minutes of work — you have options. Until it is complete, you have nothing.

4.2 Platform reporting

Every major platform has a reporting mechanism. Quality and speed of response vary wildly. The reporting mechanism for content directed at Nigerian users is typically operated from outside Nigeria, with limited indigenous-language capability and significant delays for content that does not clearly violate English-language community standards.

Despite the limitations, platform reporting is still worth using. Reasons:

- Some content is removed — particularly clear cases of explicit threats, non-consensual intimate imagery, and impersonation.
- Reports build a record. Even when individual reports do not result in removal, the cumulative record matters for civil-society advocacy with platforms and for any subsequent escalation through accredited fact-checking partners.
- Some categories of content have expedited review pathways, particularly for verified accounts and accounts in identified high-risk categories.

Platform-by-platform reporting paths

PLATFORM	HOW TO REPORT — AND WHAT WORKS
Facebook	Click the three dots on the post / message → “Find Support or Report” → select category. For impersonation, use the “Pretending to be Someone” pathway specifically — it has a faster review. For non-consensual intimate imagery, use the “Nudity or Sexual Activity → Sharing private images” pathway and check the box indicating it features you.
X (Twitter)	Three-dot menu on the post → Report post. Select the most specific category that fits. For coordinated campaigns, file individual reports on each post and add a note that you are seeing coordinated targeting. For threats, also file a separate “violent threat” report. Verified accounts receive faster review.
Instagram	Three dots on post → Report → select category. For DM harassment, hold the message → Report. For impersonation accounts, use the dedicated Instagram impersonation form (help.instagram.com → search ‘impersonation’).
WhatsApp	Open the chat → tap contact name → scroll to bottom → Report Contact and Block. Reports send the last five messages to WhatsApp. WhatsApp does not moderate content (it cannot — it is encrypted) but it does action accounts based on metadata and reports. For group harassment, leave the group, report it, and block the group admin.
TikTok	Long-press on video / comment / account → Report → select category. TikTok’s reporting flow is generally faster than other platforms for clear violations.
YouTube	Three dots under video → Report → select reason. For impersonation channels, also use the dedicated impersonation form (support.google.com → search ‘YouTube impersonation’).

When platform reporting fails

Most reports of harassment of women in Nigerian politics that do not contain explicit threats fail platform review. This is the most demoralising part of the process. When platform reporting fails, escalation pathways open through civil-society partners with accredited platform relationships — Dubawa, FactCheck Africa, CDD-WA, and others — who can refer cases through expedited partner channels. The BBYDI Rapid Response Desk (Section 4.4 below) can route cases to these partners.

4.3 Nigeria Police Force and law enforcement

Some online attacks meet the threshold for criminal complaints under Nigerian law. The relevant statutes are:

- **The Cybercrimes (Prohibition, Prevention etc.) Act 2015 (as amended):** covers cyberstalking (Section 24), online identity theft, and the unauthorised use of electronic devices. The Act has been criticised on free-expression grounds, and cyberstalking provisions have been used against journalists, so any criminal route should be considered carefully. But it remains the principal statute for online threats and harassment.
- **The Violence Against Persons (Prohibition) Act 2015 (VAPP Act):** covers a broad range of gender-based violence offences including emotional and psychological abuse. Increasingly applied in digital-violence cases at state level.
- **The Nigeria Data Protection Act 2023 (NDPA):** provides remedies where personal data has been unlawfully processed, including in doxxing cases. Civil remedies primarily; some criminal exposure exists.

How to file a criminal complaint

Filing a police complaint is a serious step with both upsides and downsides. We recommend going through these in this order:

1. **Consult a women's legal-aid organisation first.** FIDA Nigeria has chapters in most states and provides free initial consultation. They can assess whether your case is suitable for a criminal complaint and prepare you for the process. A police complaint filed without preparation typically goes nowhere; one filed with legal-aid preparation has materially better outcomes.
2. **Document thoroughly before any visit.** Bring printed copies of all evidence — screenshots, URLs, timestamps, identification of accounts where known. Bring a witness if possible. Do not rely on the officer's interpretation of digital evidence; bring it organised and labelled.
3. **File at the Police State Command level or higher, where possible.** State Cybercrime Units are typically better resourced than divisional offices for digital cases. The NPF's National Cybercrime Centre (NCCC) accepts complaints directly for serious cases.
4. **Get a Crime Diary number.** Every complaint receives a Crime Diary entry. Get the number in writing. This is what the case file is referenced by; without it, follow-up is essentially impossible.
5. **Document the police interaction.** Keep records of every visit, every officer interaction, and every response from the police. Civil-society partners can sometimes accelerate stalled cases if there is a documented record of attempted engagement.

An honest note about Nigerian law enforcement and women's complaints

Many women in Nigerian politics who have filed digital-violence complaints report that the experience itself was a second harassment — that officers minimised the complaint, asked inappropriate questions about the woman's behaviour, or did not understand the digital evidence. This is a documented pattern. The civil-society partners listed in Annex C exist in part to counter that dynamic: they accompany women to police interactions, help frame complaints in legally tractable terms, and follow up on stalled cases. Do not file a complaint alone if you can avoid it.

4.4 Civil society and legal aid pathways

In most cases, civil-society partners will be more useful than the police, at least in the first instance. They can provide:

- Verification and documentation support — particularly fact-checking organisations who can produce verdicts on disinformation directed at you;
- Platform escalation through accredited-partner pathways that bypass the standard reporting backlog;
- Legal advice and, in some cases, representation;
- Psychosocial support and crisis counseling;
- Accompaniment to police interactions where these are necessary.

Key contacts for women in Nigerian politics

- **BBYDI Rapid Response Desk:** brainbuilderedu@gmail.com — for project-affiliated cases and routing to consortium partners. From November 2026, 24/7 during peak election period.
- **FactCheck Africa:** for verification of disinformation against you. Particularly useful for content that fact-checking can authoritatively debunk.
- **Dubawa:** Nigeria's largest independent fact-checking organisation; also a member of the Nigerian Fact-Checkers' Coalition. Strong for politically-themed disinformation.
- **CDD-West Africa:** Centre for Democracy and Development; runs CDDFactCheck and has specific expertise in gendered information disorder.
- **FIDA Nigeria:** Federation of International Women Lawyers; free initial legal consultation; state chapters across the country.
- **NAWOJ:** National Association of Women Journalists; for women journalists and politically-active communicators. State branches.
- **Access Now's Digital Security Helpline:** accessnow.org/help — international, free, multilingual, 24-hour response for civil-society and politically-active individuals. Particularly strong for cases requiring technical security support.

4.5 Psychosocial support

Online harassment causes real psychological harm. The cumulative effect of sustained gendered attack is well-documented — anxiety, depression, sleep disruption, hypervigilance, and in severe cases trauma symptoms. Treating this as a security problem alone is incomplete; psychosocial support is part of the response, not an extra.

Resources:

- Mentally Aware Nigeria Initiative (MANI) — Nigeria’s leading youth-led mental health organisation; phone and online counseling support.
- She Writes Woman — mental health support specifically for women, with a 24/7 helpline.
- The Nigerian Association of Clinical Psychologists has a referral directory.
- If you are in immediate distress, the Lagos State Domestic and Sexual Violence Agency (DSVA) hotline is 08137960048 and accepts calls about online harassment as part of its remit.

If you are part of a campaign team, consider building psychosocial support into your campaign structure from the outset. Designate someone — a trusted advisor, a campaign manager, or an external counselor — whose specific role is to check in on the candidate’s wellbeing, not just her schedule.

4.6 When to involve trusted media

In some cases, going public about the attack is the right move — not as the first response, but as a deliberate escalation. Media coverage of harassment can:

- Increase platform pressure to remove content;
- Reduce the attackers’ sense of impunity;
- Build public solidarity and counter-narrative;
- Document the pattern of attacks against women in politics, contributing to the broader public record.

It can also amplify the attack, expose more of your private life, and invite a second wave of harassment from those provoked by the coverage. The choice is not obvious. Considerations:

1. **Wait until documentation is complete.** Going public without organised evidence almost always weakens the story.
2. **Work with women journalists where possible.** The CDD-WA and NAWOJ networks have relationships with reporters who specialise in gendered digital violence and will handle the story carefully.
3. **Consider the medium.** Long-form features in established outlets generally serve better than viral social-media threads. The latter often pull you into a second cycle of attention you do not control.
4. **Discuss with family before going public.** Your decision to draw public attention to attacks against you affects everyone in your life. Have the conversation in advance.

5

Documentation Strategies for Gendered Disinformation

With a single setup session of about an hour, you can build a documentation system that runs as background process for the rest of your political career.

Documentation is the single most undervalued skill in digital defence. Most women in Nigerian politics know to take screenshots. Few have a structured documentation practice that produces evidence robust enough to support platform takedown requests, fact-checker verification, legal proceedings, and the public record.

This section sets out the documentation practice the consortium recommends. It is more rigorous than the casual screenshot habit, but not difficult. With a single setup session of about an hour, you can build a documentation system that runs as background process for the rest of your political career.

5.1 Why documentation matters

Five reasons documentation is worth the effort:

1. **Evidence disappears.** Posts get deleted (by the platform, by the attacker, by accident). Accounts get suspended or repurposed. URLs change. Without contemporaneous capture, the evidence of what was done to you can simply vanish.
2. **Verification requires evidence.** Fact-checkers cannot verify a claim from a description; they need to see the original. Platforms cannot review content from a description either. Documentation is what makes everything else possible.
3. **Pattern detection requires accumulation.** A single attack can look like an unfortunate incident; a pattern of attacks documented across months tells a different story. Patterns are how civil-society partners build cases for systemic platform response.
4. **The Liar's Dividend is defeated by evidence.** When perpetrators dismiss authentic evidence as AI-generated, the defence is provenance — time-stamped, metadata-preserved, chain-of-custody-documented capture from the moment the content appeared. That defence has to be built before, not after.
5. **Documentation is empowering.** The single most demoralising aspect of sustained harassment is the feeling that it is happening to you and you have no record of what is happening. Documentation puts you back in the position of someone holding the evidence, not someone being acted upon.

5.2 The capture-and-archive method

The recommended documentation practice has three components: capture, archive, and log. Each happens within minutes of an attack landing.

Capture

The minimum capture for any incident:

- Full-screen screenshot of the offending content, with platform interface visible (so the platform is identifiable);

- Screenshot of the author's profile page (so the account is identifiable);
- Screenshot of any visible engagement metrics (likes, shares, comments, views);
- The URL of the content, copied to plain text;
- If the content is a video or audio, a screen recording of it being played;
- If the content is a thread, screenshots of the full thread, not just the offending post.

Take all of these as quickly as possible. The author may delete the content within minutes if they realise it is being noticed.

Archive

Web-archive services preserve content at a specific moment in time, independent of whether the original is later deleted. Two recommended:

- **Internet Archive's Wayback Machine:** web.archive.org → "Save Page Now." Paste the URL. The archive saves a snapshot of the page at that moment. Anyone, including fact-checkers and platforms, can later view exactly what was at that URL when you archived it.
- **Archive.today (also known as archive.ph):** an alternative web-archive service. Useful as a second copy because the Wayback Machine occasionally cannot save certain pages.

Archive every piece of significant content. The web archive's record is, in many contexts, more authoritative than a screenshot — it is harder to manipulate and easier to verify.

Log

Maintain a running log of every incident. The log entry for each incident should contain:

- Date and time you first saw the content;
- Date and time the content was posted (where visible);
- Platform;
- Account that posted it (handle, display name, follower count if relevant);
- URL;
- Web-archive URL;
- File paths to your local screenshots and screen recordings;
- A brief description in your own words of what the content is and why it is being logged;
- Severity rating (1–5) and any immediate action taken.

The log can be a simple spreadsheet. Annex D contains a printable template. The point is consistency: every incident, the same fields, the same place.

5.3 Timestamping and chain of custody

Two concepts from forensic practice are worth knowing about, because they materially affect how seriously your documentation is taken by external parties.

Timestamping

A timestamp is documentary proof that a piece of content existed at a particular moment. Three timestamps matter:

1. **The platform timestamp** — what the platform itself records as the posting time. Visible in the platform interface; usually preserved in archive captures.
2. **Your capture timestamp** — when you took the screenshot. Modern phones record this in image metadata automatically; the operating system also records file creation timestamps. Do not strip this metadata.
3. **The web-archive timestamp** — when the Wayback Machine or archive.today captured the page. This is the most independently verifiable timestamp because it comes from a third party.

Where authenticity is later contested, the convergence of these three timestamps — content posted at platform-time X, captured by you at user-time Y, archived by Wayback at archive-time Z, with Y and Z close to each other — is much harder to contest than a single screenshot in isolation.

Chain of custody

Chain of custody is the documented record of who has handled evidence between the moment it was captured and the moment it is presented. In digital documentation, the principles are:

- Original captures are stored in a write-once location — a folder you do not edit, a cloud storage account with version history, or a dedicated archive drive.
- Edits, annotations, and excerpts work on copies, not on originals.
- The log records every time evidence is shared — with whom, for what purpose, in what format.

For most documentation purposes, the chain of custody discipline does not need to be more rigorous than “originals here, copies for sharing there, log of who got what.” In legal proceedings it becomes more demanding; your legal-aid partner will guide you through that.

5.4 Metadata preservation

Digital files contain hidden information about when and where they were created, which device created them, and what was done to them. This metadata is often the difference between a screenshot that is accepted as authentic and one that is contested as fabricated.

Two practical rules:

1. **Do not strip metadata from your captures unless you have a specific reason to.** Some social-media platforms strip metadata automatically when you upload an image; this is not a problem because your local copy retains it. The local copy is the evidentiary copy.
2. **If you share a screenshot publicly, share a copy with metadata stripped** — both because your location and device details can be revealed by metadata, and because adversaries can use that information against you. But keep the original.

The two-copy principle

For every piece of documented content, maintain two copies: an evidentiary copy with full metadata, stored in your write-once archive; and a sharing copy with sensitive metadata stripped, used for any public or external sharing. The evidentiary copy is the one that matters if the authenticity of the documentation is later challenged. The sharing copy protects you from inadvertently revealing personal information through your evidence.

5.5 What goes into a documentation file

A single documentation file for a major incident — one significant enough that you might bring it to a fact-checker, a lawyer, a journalist, or law enforcement — should contain:

1. A cover note in your own words, three to five sentences, describing what the incident was and why it is significant.
2. All screenshots, ordered chronologically and labelled.
3. Screen recordings (if any), as separate video files.
4. A text file containing the URLs of the original content.
5. A text file containing the URLs of the web-archive captures.
6. Any communications you have had about the incident — emails, messages from supporters, platform reporting confirmations — as separate files or screenshots.
7. Your incident log entry, exported as a single-page PDF or text file.

Compress the whole thing into a single zipped folder, name it with the date and the platform (e.g., "2026-11-15_Facebook_impersonation"), and store it in your write-once archive. When you need to share it — with a lawyer, a fact-checker, a partner — share the whole folder, not piece by piece.

5.6 Coordinating with fact-checkers

Fact-checkers can debunk disinformation directed at you — but they need things from you. The smoother the handoff, the faster the verdict. What fact-checkers need from a complainant:

- The specific claim being made about you (not a general description of the harassment, but the precise factual claim);
- The URLs and archive URLs where the claim appears;
- Your evidence that the claim is false — documents, photographs, witness statements, official records;
- Permission to publish the verdict, with appropriate framing of your own role;
- Consent regarding what personal information of yours can be referenced in the verdict (some verdicts require referencing things — your location, your family, your employment — that you may not want widely publicised).

Approach fact-checkers with a documentation package, not a request to investigate from scratch. Their resources are limited; well-prepared submissions get acted on faster.

In the Nigerian context, the principal fact-checking organisations are members of the Nigerian Fact-Checkers' Coalition (NFC): FactCheck Africa, AFP Fact Check, Dubawa, TheCable Fact-Check, Nigerian Democratic Report (NDR), PRNigeria CableCheck, CDDFactCheck, and FactCheckHub. The BBYDI Rapid Response Desk can route your submission to the appropriate partner if you are uncertain.

6

Pre-Campaign Safety Plan

The operational synthesis: a 30-day checklist for the period before active campaigning, a 24-hour incident playbook, and the framework for building your circle of support.

This section is the operational synthesis of everything in the toolkit. The first part is a 30-day checklist for the period before active campaigning begins. The second is the 24-hour incident playbook for when an attack lands. The third is the framework for building your circle of support — the people who will help you absorb what is coming.

6.1 The 30-day pre-campaign checklist

If you have a 30-day window before the formal campaign opens, this is the work to do. The order matters: the early items reduce the surface that the later items defend.

Week 1 (Days 1–7): Audit and account setup

- **Day 1:** Run the public self-audit (Article 1, September 2026). Search your name in English and any indigenous languages you operate in. Document what is publicly visible.
- **Day 2:** Install and configure a password manager (Bitwarden recommended). Set a strong master password.
- **Day 3:** Install an authenticator app (Authy recommended) and turn on 2FA for your primary email.
- **Day 4:** Turn on 2FA for every social-media account: Facebook, X, Instagram, WhatsApp, TikTok, LinkedIn, YouTube.
- **Day 5:** Generate and save backup codes for each account. Print them; store securely; do not save only on the device you log in from.
- **Day 6:** Audit third-party app access on every account. Revoke anything you do not actively use.
- **Day 7:** Review and lock down recovery email and phone for every account. Where possible, use a dedicated recovery email.

Week 2 (Days 8–14): Account separation and platform settings

- **Day 8:** Set up a separate professional email if you do not already have one. This becomes the anchor for your political-work digital identity.
- **Day 9:** Decide on your public/personal account separation. Create separate accounts on each platform if you do not have them. Move family and personal content off public accounts.
- **Day 10–11:** Work through Section 2.3 platform-by-platform hardening. Apply every setting for every platform you use. Block strangers from DMs, group invites, and tagging on personal accounts.
- **Day 12:** Audit your friends and follower lists. Remove anyone you do not recognise, particularly from personal accounts.

- **Day 13:** Set up muted-words filters and hidden-words lists in every language you operate in. Include slurs, harassment terms, and any specific terms previously used against you.
- **Day 14:** Set up monitoring — Google Alerts for your name, Have I Been Pwned notifications for your email addresses.

Week 3 (Days 15–21): Network and documentation

- **Day 15:** Subscribe to a VPN (Mullvad or Proton VPN recommended). Install on your phone and laptop. Configure to connect automatically on public Wi-Fi.
- **Day 16:** Install Signal. Add the contacts with whom you might want to have sensitive conversations.
- **Day 17:** Set up your documentation system. Create the write-once archive folder. Set up the incident log template (Annex D). Bookmark the Wayback Machine.
- **Day 18:** Run a documentation drill. Pick an arbitrary recent post (one of your own is fine), screenshot it, archive it on Wayback, and log it. The first time should be slow; do this drill twice this week so the muscle memory builds.
- **Day 19:** Identify the civil-society partners you would call in a crisis. Save their contact details (Section 4.4) in a place you can reach quickly.
- **Day 20:** Identify your local FIDA chapter and your nearest State Cybercrime Unit. Save addresses and contact details.
- **Day 21:** Subscribe to or join women-in-politics WhatsApp or Signal groups for peer support. The first call you make when an attack lands is often to other women who have faced the same.

Week 4 (Days 22–30): Personal and family safety

- **Day 22:** Review your physical safety. Whose social-media presence reveals your home address? Family members? Old workplace bios? Ask family members to lock down their accounts; remove old bios where possible.
- **Day 23:** Talk to family members about the campaign period. Explain what kinds of attacks they should expect to see directed at you. Brief them on not engaging with attackers, not sharing personal information, and being thoughtful about what they post.
- **Day 24:** Identify a designated incident-response contact within your campaign — someone whose role includes being the person you call when something lands. This should not be the candidate; it should be someone else.
- **Day 25:** If you have children, age-appropriate conversation with them about what they might see or hear online during the campaign and how to handle it.
- **Day 26:** Mental health baseline. Set up regular check-ins with a counselor, therapist, or trusted advisor whose role is your wellbeing rather than your campaign.
- **Day 27:** Physical security review. Where do you live? Where do you work? Who has access to those places? Is there anything you would adjust knowing your information may be more public than you think?
- **Day 28:** Briefing for your team. Walk your campaign manager and core team through this section. Make sure the documentation discipline and incident-response protocols are shared, not yours alone.
- **Day 29:** Test runs. Simulate what you would do in the first hour of a major incident. Identify gaps; fix them.
- **Day 30:** Final calm review. Take an evening for yourself. The work is done. The campaign begins.

6.2 The 24-hour incident response playbook

Use this when an attack lands. Work through it in order. Do not skip steps. Do not improvise. The instinct to react is the enemy of the response.

TIME	ACTION	DETAIL
0–5 min	Pause	Do not reply. Do not delete. Do not call anyone yet. The first five minutes are for absorbing what is happening and not making it worse. Breathe.
5–30 min	Document	Capture every piece of the attack: screenshots, URLs, screen recordings, account information. Archive to Wayback Machine. Log everything. The documentation must be complete before you act.
30–60 min	Tell one person	Contact your designated incident-response contact. Not to fix it — to share the load. Brief them, share the documentation folder, and decide together what comes next.
1–4 hrs	Triage and report	Assess severity: is this a single incident, the start of a coordinated campaign, or a security threat? File platform reports. If criminal threshold met, brief your legal-aid partner. If physical safety implicated, consider relocation.
4–12 hrs	Escalate strategically	If platform reports unlikely to suffice, escalate through accredited civil-society partners (Dubawa, FactCheck Africa, CDD-WA). If disinformation, request a verification verdict. Continue documentation as the attack evolves.
12–24 hrs	Communications	Decide whether and how to make a public statement. If you do, work with women journalists where possible. Do not respond to the attackers directly. Do not amplify the content by quoting it. Frame the statement in your own terms.
24 hr+	Aftercare	Check in on yourself. Check in on family members. Schedule a follow-up with your counselor. Update your documentation file with everything that has happened. Plan the next 72 hours of monitoring.

Three things never to do in an incident

First: never reply directly to the attacker. Replies amplify the content algorithmically and give the attacker the engagement they wanted. **Second:** never delete your own content in panic. If you decide some of your content is now unsafe, archive it (download a copy) before deleting, so you retain your own record. **Third:** never make security decisions alone in the first 24 hours. The incident-response contact role exists precisely so you have a second mind on every consequential decision.

6.3 Building your circle of support

The most consistent finding in research on women who have weathered sustained online attacks is this: the women who came through best were the ones who built their support structure before they needed it. The women who suffered the most acute psychological harm were typically the ones operating alone.

Your circle of support should include, at minimum, the following roles. They can be one person each or, ideally, more than one.

- **The incident-response contact:** the person who picks up the phone when an attack lands. Their role is to share the cognitive load, hold the documentation folder, and help you decide on next steps. This is not a casual friend; it is someone whose specific commitment is to be reachable in a crisis.

- **The legal contact:** a women's-rights lawyer or civil-society legal-aid partner who you have already met and briefed, so that if you need to file a complaint or seek a restraining order, you are calling someone who already knows you.
- **The mental-health contact:** a counselor, therapist, or trusted advisor whose role is your wellbeing rather than your campaign. The strategic clarity you need under attack comes from being emotionally regulated; the mental-health contact's job is to help you stay so.
- **The peer contact:** another woman in Nigerian politics or civil society who has weathered something similar. The shared experience is, for many women, the most important single source of strength. Find her before you need her.
- **The family contact:** the family member who knows what you are doing and why, who will not panic, and whose role is to be the steady presence. If you have a partner or close family, this is usually them. Brief them in advance.

Build the circle in the 30 days before the campaign begins. Have one explicit conversation with each person about what their role would be. It is uncomfortable; the conversation is also one of the most valuable single things you can do for yourself in this period.



Annex A — Glossary

2FA	Two-Factor Authentication. A login requiring both a password and a second factor (a code from an app, or a hardware key).
Bot	An automated account, often used in coordinated campaigns to amplify content. Bot networks can include hundreds or thousands of accounts.
CIB	Coordinated Inauthentic Behaviour. The organised manipulation of online discourse — synchronised posting, link-sharing, hashtag amplification — designed to misrepresent popular sentiment.
Deepfake	Synthetic media (typically video) produced by AI to depict a person saying or doing something they did not say or do.
Doxxing	The public release of private information about a person, often as a vector for harassment or threats.
End-to-end encryption (E2EE)	Encryption in which only the sender and recipient can read messages. The platform itself cannot. WhatsApp, Signal, and iMessage use E2EE.
Gendered disinformation	False information deployed against a woman, drawing on gender stereotypes to undermine her credibility or fitness for office.
Hardware key	A physical device (such as a YubiKey) that proves your identity to platforms during 2FA. The strongest form of 2FA.
Liar's Dividend	The dynamic by which the existence of AI-generated content allows perpetrators to dismiss authentic damaging evidence as fabricated.
Metadata	Hidden information embedded in digital files: when they were created, on what device, where, and what was done to them. Often forensically significant.
NDPA	Nigeria Data Protection Act 2023. The principal Nigerian statute governing personal data, including online harassment cases where personal data is misused.
NFC	Nigerian Fact-Checkers' Coalition. The professional network of Nigerian fact-checking organisations including Dubawa, FactCheck Africa, AFP Fact Check, and others.
OGBV	Online Gender-Based Violence. Harassment, threats, image-based abuse, and other harms directed at a person because they are a woman, enabled by digital technologies.
Password manager	Software that generates and stores unique passwords for every account, secured behind a single master password.

Phishing	An attack in which the attacker imitates a legitimate service to trick you into entering your credentials.
SIM swap	An attack in which the attacker convinces your mobile operator to transfer your phone number to a SIM they control.
VPN	Virtual Private Network. A service that encrypts your traffic and routes it through a remote server, hiding your IP address from the services you visit.
Wayback Machine	The Internet Archive's web-archive service. Preserves snapshots of web pages at specific moments, independent of whether the original is later deleted.



Annex B — Quick-Reference Cards

Print these. Carry one in your bag; tape one to your laptop; share with your team.

CARD 1: THE FIRST 30 MINUTES OF AN INCIDENT

1. Pause. Do not reply. Do not delete.
2. Screenshot the content, the account, and the engagement metrics.
3. Copy the URL. Archive it on web.archive.org.
4. Log the incident: time, platform, account, URL, severity.
5. Call your incident-response contact. Brief them.
6. Decide on next steps together. Do not improvise alone.

CARD 2: ESSENTIAL ACCOUNT HARDENING

- ✓ Password manager installed; unique strong password on every account.
- ✓ Authenticator-app 2FA on email, all social media, cloud storage, banking.
- ✓ Backup codes printed and stored physically. Never SMS-only 2FA.
- ✓ DMs locked down on all platforms. Strangers cannot reach you directly.
- ✓ Recovery email is itself hardened (2FA on). Recovery phone secured.
- ✓ Third-party app access audited; unused apps revoked.
- ✓ Personal and political accounts separated where possible.

CARD 3: DOCUMENTING AN ATTACK

Capture: Full screenshot, profile screenshot, engagement screenshot. URL copied. Screen recording if video / audio.

Archive: web.archive.org → “Save Page Now” → paste URL. Backup: archive.today.

Log: Date / time seen. Platform. Account. URL. Archive URL. Description. Severity 1–5.

Folder name: YYYY-MM-DD_platform-brief-description.zip → write-once archive.



Annex C — Nigerian Resource Directory

All resources current as of June 2026. Verify contact details before relying on them in a crisis.

Project consortium

- **Brain Builders Youth Development Initiative (BBYDI):** brainbuilderedu@gmail.com | +234 814 746 4597 | www.thebrainbuilders.org
- **BBYDI Rapid Response Desk:** from November 2026, 24/7 during peak election period. Contact via brainbuilderedu@gmail.com.
- **FactCheck Africa:** consortium partner; verification of disinformation against you.

Fact-checking organisations

- **FactCheck Africa:** <https://factcheckafrica.net/>
- **Dubawa:** dubawa.org
- **AFP Fact Check:** factcheck.afp.com Nigerian coverage.
- **TheCable Fact-Check:** factcheck.thecable.ng
- **Nigerian Democratic Report (NDR):** ndr.org.ng
- **CDDFactCheck (Centre for Democracy and Development); FactCheckHub:** factcheckhub.com

Women's rights, legal aid, and gender-violence response

- **FIDA Nigeria (Federation of International Women Lawyers):** fidanigeria.org — free initial legal consultation; state chapters across the country.
- **NAWOJ (National Association of Women Journalists):** for women journalists and politically-active communicators; state branches.
- **Lagos State DSVa (Domestic and Sexual Violence Agency):** 08137960048 — accepts calls about online harassment as part of remit.
- **WARDC (Women Advocates Research and Documentation Centre):** long-standing women's rights organisation; legal advocacy and documentation support.
- **Women Empowerment and Legal Aid (WELA):** legal aid for women's rights cases including digital violence.

Mental health and psychosocial support

- **Mentally Aware Nigeria Initiative (MANI):** mentallyaware.org — phone and online counseling support.
- **She Writes Woman:** shewriteswoman.org — 24/7 helpline; mental-health support specifically for women.
- **Asido Foundation:** asidofoundation.com — mental health awareness, advocacy, and access to care.

International support

- **Access Now Digital Security Helpline:** accessnow.org/help — 24-hour multilingual response; technical security support.
- **Committee to Protect Journalists (CPJ) Emergencies:** cpj.org/emergency-response — for journalists facing threats.
- **Front Line Defenders:** frontlinedefenders.org — emergency support for human rights defenders, including women political activists.

Government and law enforcement

- **Nigeria Police Force National Cybercrime Centre (NCCC):** accepts complaints directly for serious cybercrime cases.
- **INEC (Independent National Electoral Commission):** inecnigeria.org — for election-period violations specifically.
- **NDPC (Nigeria Data Protection Commission):** ndpc.gov.ng — for NDPA-related complaints, including unauthorised use of personal data in doxxing cases.



Annex D — Reporting Templates

T1 Template 1 — Incident Log Entry

Incident ID	YYYY-MM-DD-NN (assigned at logging)
Date / time of incident	[when the content was posted, where visible]
Date / time first seen	[when you became aware]
Platform	[Facebook / X / Instagram / WhatsApp / TikTok / YouTube / other]
Account / author	[handle, display name, follower count if relevant, verified status]
Original URL	[paste here]
Archive URL (Wayback Machine)	[paste here]
Type of content	[text / image / video / audio / mixed]
Category	[direct harassment / gendered disinformation / doxxing / impersonation / threats / other]
Severity (1–5)	[1 = minor, single occurrence 5 = serious threat or coordinated campaign]
Brief description	[three to five sentences in your own words]
Local files captured	[list of screenshot / recording filenames in your archive]
Actions taken	[platform report filed / civil-society partner contacted / police filed / public statement / no action yet]
Follow-up needed	[any open items; next-check date]

T2 Template 2 — Fact-Check Referral Form

Use this when submitting an incident to a fact-checking partner.

Submitter name	[your name]
Submitter contact	[email and / or phone]
Specific claim being made	[the exact factual claim, in one sentence]

Where the claim appears	[URLs and archive URLs]
Why the claim is false	[evidence supporting the rebuttal — documents, photographs, official records]
Supporting documents attached	[list of attached files]
Consent for publication	[can the verdict reference you by name? are there details you would prefer not to be referenced?]
Urgency	[is there a time-sensitive context — upcoming event, ongoing campaign, escalating threat?]

This toolkit is part of the Strengthening Digital Integrity and Inclusive Participation for Nigeria 2027 project, implemented by Brain Builders Youth Development Initiative (BBYDI) and FactCheck Africa, with the support of the Digital Democracy Initiative (DDI) and CIVICUS. It is distributed under a Creative Commons Attribution-NonCommercial 4.0 licence — please share, translate, and adapt, with credit.

This is a living document. We update it as platforms change, as Nigerian law evolves, and as the threat surface shifts. The current edition is always available on request from brainbuilderedu@gmail.com.

— END OF TOOLKIT —



Email: brainbuilderedu@gmail.com **Tel:** 07068775529

Headquarters: 2 Catchment Road, Opposite Forest, Along Sydney Restaurant, GRA, Ilorin

Abuja Address: No. 12 T.O.S. Benson Crescent, Utako Abuja, 900108, FCT

Cameroun Address: Yaoundé- Montee Jouvence, Patmos Church Street 8.560

US Address: 1301 S Bowen Rd STE 450 Arlington TX 76013

www.thebrainbuilders.org