

# HerSafeSpace Digital Safety Manual





# HerSafeSpace Digital Safety Manual

---

SUPPORTED BY



## Disclaimer

This manual is for informational and educational purposes only. It does not offer legal, medical, or psychological advice and should not replace professional support where needed.

While care has been taken to ensure accuracy, HerSafeSpace is not liable for any outcomes resulting from the use of this material. Mention of tools or services does not imply endorsement.

Use this guide as a supportive resource, not a substitute for expert help. Your safety journey is personal—proceed with care and choose what works best for you.

# welcome

## to **HerSafeSpace**

### Digital Safety Manual

---

Dear Reader,

Welcome to HerSafeSpace, a space designed with you in mind. It doesn't matter if you've picked up this manual out of curiosity, fear, experience, or hope; we want you to know something right from the start:

You are not alone.

You are not "too sensitive."

And you are not powerless.

In today's world, much of our lives, including our learning, work, friendships, and even love, take place online. But with that connection comes risk. From unwanted messages to full-blown blackmail, from trolling to threats, the internet can become a dangerous place, especially for women, girls, and marginalised communities.

That's why HerSafeSpace exists.

We created this manual to:

**Help you understand online gender-based violence (OGBV) in all its forms**

**Teach you how to protect yourself and others**

**Show you where to go for help when things get tough**

**And guide you on a path of healing, allyship, and leadership**

You'll find practical steps, honest conversations, real-life tools, and powerful stories inside. We've kept the language simple and the tone human, because safety shouldn't feel complicated.

So flip through these pages at your own pace. Share them with a friend. Teach your sister. Talk to your brother. Pass it on.

Let HerSafeSpace be your partner in reclaiming your power, dignity, and peace, one click, one choice, one boundary at a time.

With care,

**The HerSafeSpace Team**

# Chapter 1: Why This Manual Matters



The internet can be a powerful place. A space to learn, connect, grow your business, raise your voice, and find community. But for many women and girls across West Africa, being online also comes with fear, harassment, and abuse.

Maybe you've been followed by a stranger on Facebook.

Maybe someone threatened to leak your private photos.

Maybe you were insulted just for speaking your mind online.

You're not imagining things, and you're not alone.

## Online Gender-Based Violence is Real.

Across Nigeria, Ghana, Benin, Togo, and Cameroon, thousands of women and girls face some form of online harm every day. It comes in different forms:

- 1 People sharing your pictures without permission.
- 2 Fake accounts spreading lies about you.
- 3 Messages filled with threats or sexual harassment.
- 4 Friends or partners stalking your every move online.

It Is Your Digital Safety Companion. It's your practical, personal, and powerful guide to navigating the online world safely. Inside, you'll find:

1

**Tips to protect yourself and your accounts.**

2

**Real advice on what to do if you're being harassed or blackmailed.**

3

**Tools you can use, even if you have low data or an old phone.**

4

**Ways to heal, find support, and help others.**

Whether you're a student, entrepreneur, activist, or just someone who wants peace of mind online, this manual is for you.

We built this with you in mind:

•

**It's written in clear, everyday language.**

•

**It includes real examples from real women.**

•

**It shares free tools you can start using right now.**

•

**It talks about healing and mental health, not just tech stuff.**

•

**It also shows how men can become part of the solution.**

You deserve to feel safe, both offline and online. And while we can't fix the internet overnight, we can give you the knowledge, tools, and confidence to protect yourself and support others.



## Chapter 2:

# Understanding Online Gender-Based Violence

Let's start with something clear: online violence is real violence.

Just because it happens on a screen doesn't make it any less painful or harmful. It can ruin reputations, destroy confidence, affect mental health, and in some cases, even put lives at risk. But what exactly does online gender-based violence mean?

# What Is Online Gender-Based Violence (OGBV)?

Online Gender-Based Violence (OGBV) happens when someone uses the internet, social media, or digital tools to threaten, harass, shame, or abuse another person because of their gender.

It mostly targets women, girls, and LGBTQ+ people. And it can come from strangers, friends, family, classmates, partners, even people you've never met.

## Where Does It Happen?

Sadly, it can happen anywhere online. But some platforms are more common than others. These include:

- **WhatsApp** – where private messages, pictures, and groups can be misused.
- **Facebook & Instagram** – where public shaming, fake accounts, and harassment are frequent.
- **TikTok** – where viral videos can lead to bullying or unwanted attention.
- **Twitter/X** – where trolling, impersonation, and hate speech are widespread.

Sometimes, the abuse is public. Other times, it's hidden in DMs, secret groups, or disappearing messages.

## Why Does This Happen So Often?

There are many reasons:

- **Power and control** – just like offline abuse.
- **Patriarchy and sexism** – many still believe women shouldn't speak up or take space online.
- **Weak laws** – in some places, the law fails to adequately protect victims.
- **Digital illiteracy** – many don't know how to protect their accounts or report abuse.
- **Shame and silence** – victims are often blamed, not supported.

## What Does It Look Like?

OGBV takes many forms. Here are some of the most common:



### Harassment and Bullying:

Constant insults, sexual messages, or threats in your inbox or comments.



### Non-consensual Image Sharing (NCII):

Sharing someone's private photos or videos without permission. Often called "revenge porn."



### Stalking and Surveillance:

Monitoring your posts, checking your online movements, or using fake accounts to watch you.



**Doxxing:** Posting your personal details (like your phone number or address) online to shame or endanger you.



**Impersonation:** Someone creates a fake account pretending to be you to scam others or damage your image.



**Sextortion:** Someone blackmails you with intimate content, often threatening to share it unless you pay or do something.



**Online "Kito" or Outing:** Tricking LGBTQ+ people into meeting and then extorting or exposing them.

## Why It's So Dangerous

The effects of OGBV are very real:

- Depression, anxiety, fear
- Dropping out of school or quitting jobs
- Losing self-esteem or trust in people
- Even feeling suicidal

And when victims report it, they're sometimes ignored, shamed, or threatened even more.



## Chapter 3:

# **Who Is Most at Risk and Why**

Online violence can happen to anyone. But the truth is, some people are more targeted than others, just because of who they are, what they do, or what they believe in.



## Young Women and Teenage Girls

If you're a girl in secondary school or a young woman on campus, you've probably seen or faced some form of online abuse.

- Random men sending disturbing messages.
- Classmates sharing your photos without asking.
- People mocking your posts just because you're outspoken.

You're seen as "easy targets" and sometimes, you don't even know it's abuse until it's too late.



## Women Who Speak Up

If you're an activist, journalist, businesswoman, or public figure, being visible online can come at a cost.

- Trolls attack your looks, your voice, your family.
- Men flood your comments with abuse or threats.
- Some try to silence you with shame or fake scandals.

The more power you have, the more some people try to take it away.



## Rural Women and Girls

Being far from cities doesn't mean you're safer. Sometimes, it means you have less support.

- Poor network makes it hard to report or get help.
- Many don't know how to use safety tools or even what rights they have.
- Abuse is more likely to be handled "privately," with silence and shame.



## Women with Disabilities

Online, people with disabilities face double discrimination:

- Being mocked, fetishised, or excluded
- Struggling with apps or websites that aren't accessible
- Lacking tools like screen readers, captioning, or audio support

If your device isn't designed with you in mind, how can you protect yourself?



## Women with Religious or Cultural Visibility

Wearing a hijab. Posting in a local language. Expressing cultural beliefs. These simple acts can trigger hate and harassment, especially when stereotypes come into play. You're punished not just for being online, but for being yourself.

## Why This Matters

When we know who is at risk, we can create tools that actually protect them.

This manual was designed with you in mind, whether you're a rural teenager, a young activist, or a quiet learner who just wants to enjoy the internet in peace.

Everyone deserves to feel safe online. No exceptions.

## Chapter 4:



# Privacy Basics — Locking Down Your Digital Life

Most of us are online every day. We chat, post, share, and scroll. But very few of us stop to ask: “Is my digital life really safe?”

Just like you lock your front door at night, you should be locking your accounts, devices, and digital identity. It doesn’t mean you’re hiding something; it means you’re protecting yourself.

### Why Digital Privacy Matters

When your online life isn’t secure, someone else can:

- Steal your private photos or chats.
- Pretend to be you online.
- Watch your activity without your knowledge.
- Send threats or blackmail you.
- Spread lies that hurt your reputation or safety.

And many times, it starts with just one weak password or one click on the wrong link.

## 5 Simple Ways to Protect Yourself Online

### 1. Use Strong Passwords and Don't Repeat Them

- Avoid easy passwords like “123456” or “yourname2024”.
- Combine capital letters + numbers + symbols (e.g., Joy@Life234)
- Use different passwords for different accounts.

### 2. Turn On Two-Factor Authentication (2FA)

- 2FA is like a second lock on your door.
- It sends a code to your phone or email when someone tries to log in.
- You'll find this in your account security settings.

Platforms like WhatsApp, Facebook, Gmail, and Instagram all support it.

### 3. Review Your Privacy Settings Often

Go to your account settings and check:

- Who can see your posts?
- Who can send you friend requests or messages?
- Are you sharing your location without knowing it?

Set your accounts to “friends only” or “private” wherever possible, especially on Facebook, Instagram, and TikTok.

### 4. Be Careful What You Click

- Avoid clicking links from strangers or suspicious DMs.
- Don't download unknown apps or files.
- Watch out for “free giveaways” many are just scams.

Warning: One click can give someone access to your entire phone.

### 5. Log Out of Shared Devices

If you use a public phone or cybercafé:

- Always log out of your accounts.
- Never save your passwords on shared computers.
- Clear your browser history after use.

Even at home, if others use your phone, set up a screen lock and protect sensitive apps with a pin.

## Platform-Specific Safety Tips

### WhatsApp

- Turn on 2-step verification (Settings > Account > Two-step verification)
- Block and report suspicious contacts.
- Avoid forwarding sensitive messages or photos.

### Facebook

- Use Privacy Checkup in Settings.
- Hide your friend list.
- Limit who can tag you in posts.

### Instagram

- Switch to a private account.
- Use comment filters to block abusive words.
- Turn off location tagging.

### Google / Gmail

- Set up recovery options (phone & email).
- Review your Google account security dashboard.
- Don't ignore warning emails from Google.

### Remember...

Privacy isn't about being secretive; it's about being in control. Even if you're not “tech-savvy,” you can take small steps that make a big difference. You deserve to feel safe not just on the street, but also on your screen.

## Chapter 5:



# Social Media Survival Guide

Social media is where we live, laugh, learn, and connect. But it's also where many women and girls face bullying, blackmail, and abuse. So how do you stay visible without becoming a target?

This chapter gives you smart, simple steps to protect yourself and take control of your online presence.

### First, Know the Risks

Different platforms come with different dangers:

- **Facebook:** Fake profiles, public tagging, malicious comments.
- **Instagram:** Unwanted DMs, photo theft, impersonation.
- **WhatsApp:** Group leaks, message forwarding, stalking.
- **TikTok:** Viral bullying, body-shaming, sexualised comments.
- **Twitter/X:** Dogpiling, hate speech, doxxing.

Many abusers use screenshots, fake accounts, or private chats to harm victims. But you can fight back by getting smart, not silent.

# 5 Simple Ways to Protect Yourself Online

## Step 1: Manage Your Digital Footprint

Ask yourself:

- What can strangers learn about me in 30 seconds?
- Can someone find where I live, school, or work from my posts?

Do This:

- Avoid sharing your exact location or daily routine.
- Don't post everything in real time; delay your uploads.
- Blur or hide details like uniforms, ID cards, and street names.
- Remove your phone number and email from public profiles.

Tip: Google yourself once in a while. See what others can find.

## Step 2: Control Who Can See and Contact You

On Facebook:

- Set your posts to "Friends only."
- Limit who can send you friend requests.
- Use the "Timeline Review" tool to approve tags.

On Instagram:

- Switch to a private account.
- Block unknown followers and spam accounts.
- Restrict users who make you uncomfortable; they won't know.

On WhatsApp:

- Hide your profile photo from non-contacts.
- Turn off "Last Seen" and "Read Receipts" if needed.
- Exit toxic or untrusted groups silently.

## Step 3: Block, Report, and Delete

You don't owe anyone your space, time, or peace of mind.

If someone is making you uncomfortable:

- Block them. It's not rude, it's smart.

- Report the account to the platform.
- Delete triggering messages but always screenshot first if there's abuse.

## Step 4: Share Safely

Before you post, pause and ask:

- Is this something I'm okay with strangers seeing?
- Could this post be misused or misinterpreted?
- Am I giving away more than I realise?

Rule of Thumb: If you wouldn't shout it in a crowded room, think twice before posting it online.

## Step 5: Think Twice Before Engaging

Not every comment needs a reply. Not every troll deserves your attention. Trolls want reactions. Don't give them the satisfaction. Silence, blocking, or reporting are powerful choices.

## Bonus Tips

- Avoid arguing with strangers on controversial posts, especially on public platforms.
- Don't click random links, even from friends (they might've been hacked).
- Regularly review your "tagged photos" and mentions.
- Join trusted, safe online communities. Avoid toxic spaces.

## You Deserve to Be Seen Safely

You have every right to post, create, express, and thrive online. Being safe doesn't mean being silent. It means being smart, aware, and in control.

## Chapter 6:



# Recognising and Responding to Abuse

Sometimes, online abuse starts small. A strange message, a rude comment, a joke that doesn't feel like a joke. Other times, it hits hard and fast. A threat, a leaked photo, a fake profile pretending to be you.

Whether it builds up slowly or strikes suddenly, the first step is recognising it for what it is: Abuse. Violation. Violence.

## How to Know You're Being Abused Online

If any of this sounds familiar, you're not overreacting:

- Someone constantly sends you unwanted messages, especially sexual or threatening ones.
- Someone shares your private photos or videos or threatens to.
- A fake account is using your name or photos.
- You're being shamed, mocked, or bullied in public comments.
- Someone is stalking your activity, liking old posts, tracking your location, or watching your stories within seconds.
- A person demands money, favours, or silence in exchange for not leaking something about you.

These are not "normal online problems." They are forms of violence.

# What to Do — Step by Step

Here's a quick emergency plan when something goes wrong:

## 1. Breathe and Pause

You might feel shocked, angry, scared, or numb. That's normal. Before reacting, give yourself a moment to breathe. You're not alone, and you have options.

## 2. Collect Evidence

Even if you plan to block or delete, always save proof first:

- Take clear screenshots (include names, timestamps, messages).
- Save links to posts or profiles.
- Record voice notes or videos if necessary.
- Store them in a safe folder or email them to yourself.

## 3. Block and Report the Abuser

Every platform has tools to block or report, use them.

- On WhatsApp, you can block and report directly in the chat.
- On Facebook/Instagram, you can restrict, block, and report with a few taps.
- On Twitter/X, use the report function for harassment, hate speech, or impersonation.

Don't argue or warn them. Just block, report, and move on.

## 4. Tell Someone You Trust

This might be hard, but you don't have to go through it in silence.

- Tell a trusted friend, sibling, or mentor.
- Reach out to a local women's group or hotline.
- If it involves threats, blackmail, or NCII (non-consensual image sharing), seek legal or NGO help right away.

## 5. Know When to Escalate

Some situations need more than blocking.

Escalate when:

- You feel unsafe offline (e.g., someone threatens to find you).
- Your private content has been shared publicly.
- You're being blackmailed or extorted.
- Someone is impersonating you or ruining your reputation.

In these cases, report to:

- Local police (if safe to do so).
- A legal clinic or women's rights organisation.
- Platforms like HerSafeSpace, Take Back the Tech, or Digital Rights Africa.

## What NOT to Do

- Don't confront the abuser alone.
- Don't delete messages before you save evidence.
- Don't stay silent out of shame. Abuse thrives in silence.
- Don't feel pressured to "just ignore it", your feelings are valid.

## Remember...

You have the right to be online without fear. You deserve help. You deserve respect. You deserve peace.

## Chapter 7:

# Know Your Rights



When someone harasses, blackmails, or abuses you online, it's not “just drama” or “social media wahala.” It's a violation of your rights.

You have the right to:

- Be safe — online and offline
- Speak up without fear
- Keep your private life private
- Report abuse and expect action
- Let's break it down country by country.

## Nigeria

### What the law says:

- The Cybercrimes Act (2015) makes cyberstalking, blackmail, and identity theft a criminal offence.
- Section 24 specifically protects victims from online threats, bullying, and revenge porn.
- The Violence Against Persons (Prohibition) Act (VAPP) recognises psychological and digital violence.
- You can report to:
  - National Human Rights Commission
  - Nigeria Police Force – Cybercrime Unit
  - NGOs like WARIF, Stand to End Rape, or TechHer

## Benin

### What the law says:

- The Digital Code of Benin (2018) punishes cyberstalking, identity theft, and digital blackmail.
- Laws also protect minors from online abuse.
- You can reach out to:
  - Autorité de Protection des Données Personnelles (APDP)
  - Local women's rights groups or legal aid clinics.

### What You Can Do No Matter Where You Live

- Know the law in your country, even if it's not perfect.
- Keep records of abuse, including screenshots, links, and messages.
- Report to multiple places — the police, your school, your workplace, or local CSOs.
- Find support — you don't have to go through the system alone.

### You Deserve Justice

Even if the law doesn't always work the way it should, knowing your rights is your first line of defence.

## Ghana

### What the law says:

- The Cybersecurity Act (2020) and Criminal Offences Act criminalise cyberbullying, sexual extortion, and digital threats.
- You can report online abuse to:
  - Ghana Cyber Security Authority
  - Domestic Violence and Victim Support Unit (DOVVSU)
  - NGOs like WILDAF Ghana or FIDA

## Togo

### What the law says:

- Togo's Law on Cybercrime (2018) covers online threats, image misuse, and fraud.
- The Penal Code prohibits digital sexual harassment.
- You can report to:
  - Haute Autorité de l'Audiovisuel et de la Communication (HAAC)
  - Local organisations like AFJN Togo

## Cameroon

### What the law says:

- The Cybersecurity and Cybercrime Law (2010) covers hacking, online abuse, and digital privacy.
- Defamation and blackmail are criminal offences, including online.
- You can report to:
  - National Agency for Information and Communication Technologies (ANTIC)
  - NGOs like Reach Out Cameroon

## Chapter 8:

# How to Report and Get Help



If you've been harassed, stalked, blackmailed, or attacked online, your first thought might be:

***"Who do I tell?"***

***"Will anyone even help me?"***

You need to know where to go and what steps to take. This chapter breaks it all down.

### Step 1: Gather Your Evidence

Before reporting anything, collect solid evidence. Without it, most cases won't go far.

Save:

- Screenshots of messages, images, or comments (include timestamps & usernames).
- Links to profiles, posts, or shared content.
- Voice notes, call logs, or threatening DMs.
- Any contact information from the abuser (phone number, email, username).

Tip: Back up your evidence in the cloud or email it to yourself. Don't keep everything on just one device.

### Step 2: Report to the Platform

Most platforms have built-in tools for reporting abuse. Here's how:

#### WhatsApp

- Open the chat > Tap the name > Scroll down to "Report."
- You can also block and delete.

#### Facebook

- Tap the three dots on any post or profile > "Find Support or Report."
- Use the "Support Inbox" to track your report.

#### Instagram

- Tap the three dots > "Report" > Choose the reason (e.g., harassment, impersonation).
- Block and restrict as needed.

#### Twitter/X

- Click the three dots > "Report Tweet" or "Report Account."
- Choose the appropriate reason (abuse, hate speech, etc.)

#### TikTok

- Tap the share icon on the post > "Report."
- Block and restrict comments on your own content.

Report early and often. The more reports they receive, the faster they may act.

### Step 3: Report to Authorities or Legal Aid

This depends on where you live and the nature of the abuse.

Here's where to go by country:

#### Nigeria

- Cybercrime Unit – Nigeria Police Force
- National Human Rights Commission
- NGOs: WARIF, TechHer, Mirabel Centre, Brain Builders Youth Development Initiative (BBYDI), Rising Child Foundation (RCF)

#### Ghana

- Cyber Security Authority
- DOVVSU (Domestic Violence Unit)
- NGOs: WiLDAF, FIDA Ghana

#### Benin

- Autorité de Protection des Données Personnelles (APDP)
- Legal aid from women's networks=

#### Togo

- Haute Autorité de l'Audiovisuel et de la Communication (HAAC)
- NGOs working on gender or media rights

#### Cameroon

- ANTIC (National Agency for ICT)
- NGOs like Reach Out Cameroon

### Step 4: Seek Emotional and Legal Support

Dealing with abuse is tough, emotionally and mentally. You don't have to go through it alone.

Look for:

- Support groups (online or offline)
- Mental health hotlines or safe spaces
- Legal clinics offering free help for survivors
- Community-based organisations who know your local laws and rights

Some NGOs will escort you to report, help draft a legal letter, or link you with a counsellor.

### **Step 5: Use Survivor-Support Tools**

Here are a few helpful tools you can access anytime:

- HerSafeSpace WhatsApp Bot – For advice, reporting tips, and emotional support.
- Red Dot Foundation – For tracking and reporting sexual harassment.
- Take Back the Tech! – Global network with resources on OGBV.
- Digital First Aid Kit (by Access Now) – Step-by-step help for digital emergencies.

### **Reporting Is Brave, Not Shameful**

Many survivors stay silent because of fear, shame, or threats.

But remember:

- You did not cause this.
- You are not weak for asking for help.
- You don't owe your abuser anything but you do owe yourself peace and protection.

## Chapter 9:



# Healing and Self-Care After Abuse

Online abuse doesn't end when you block someone. The pain can linger in your thoughts, your body, and your confidence. But here's the truth no one tells enough: Healing is possible. You can feel safe again. You can feel strong again. You can reclaim your joy.

This chapter is about helping you get there gently, one step at a time.

### First, Understand the Impact

Online Gender-Based Violence (OGBV) can lead to:

- Anxiety, fear, or constant worry
- Trouble sleeping or focusing
- Feeling ashamed, angry, or numb
- Isolation — pulling away from friends or online spaces
- Loss of trust in people or platforms
- Depression or thoughts of self-harm (in severe cases)

# 7 Ways to Start Healing

## 1. Talk to Someone You Trust

Share your experience, even if you just say, “Something happened, and I don’t feel okay.”

- A close friend, sibling, teacher, or mentor
- A therapist or counsellor
- A community organisation or support group

Talking helps you release the weight.

## 2. Limit Screen Time for Now

It’s okay to take a break from social media, messaging apps, or even your phone.

- Turn off notifications
- Delete triggering apps (you can come back when ready)
- Spend time offline with people or activities you love

## 3. Create a Safe Online Space

When you’re ready to go back online:

- Set stricter privacy settings
- Mute or block harmful words/accounts
- Follow pages that uplift and inspire you
- Avoid toxic or triggering discussions
- You have the right to curate peace.

## 4. Rebuild Your Confidence

- Write affirmations like: “I am not what happened to me.”
- Take back control: Change passwords, report accounts, clean your digital space.
- Celebrate small wins — even getting out of bed is a victory.

Keep a journal to track your healing. It helps more than you think.

## 5. Join a Survivor Circle

You’re not alone and you’re not the only one.

- Look for local or online support groups
- Share your story (if you feel ready)
- Listen to others and draw strength from them

There’s power in community.

## 6. Seek Professional Help

Mental health is a right.

- If you’re feeling overwhelmed, speak to a trained counsellor.
- Many NGOs now offer free or low-cost therapy.
- You can also access anonymous mental health support apps or helplines.

## 7. Give Yourself Grace

- Healing isn’t a straight line. Some days will be hard. Others will be brighter.
- Don’t rush yourself. Don’t shame yourself.
- Just keep moving at your own pace.

## You Are Not What Happened to You

You are not the abuse.

You are not the screenshots.

You are not the shame.

You are a survivor.

A fighter.

A light that’s still shining and will shine even brighter.

## Chapter 10:



# Becoming a Digital Safety Champion

By now, you know how to protect yourself. But what if you could protect others too?

Here's how to become a true Digital Safety Champion in your school, group, or community.

### 1. Share What You've Learned

Use your voice, online or offline, to educate others.

- Post safety tips on WhatsApp, Instagram, or Twitter/X.
- Host a mini session at your school, youth group, or religious centre.
- Help friends review their privacy settings or block abusers.

### 2. Be a Safe Person for Others

Sometimes, all someone needs is one friend who believes them.

- Let others know they can talk to you if they face abuse.
- Don't judge, blame, or ask "what did you do?"
- Help them document and report what happened.

Know local organisations and hotlines you can refer people to.

### 3. Advocate for Better Systems

Want real change? Speak up where it matters.

- Tell your school to include digital safety in orientation programs.
- Encourage youth groups to host awareness events.

- Join or create a campaign against online violence.

Use your story. Use your strength. Use your knowledge.

### 4. Help Build Safer Tech Spaces

You don't need to be a "techie" to make tech better.

- Give feedback to apps or platforms when something doesn't feel safe.
- Suggest tools for reporting, blocking, or filtering.
- Join youth tech communities or training programs — your ideas matter.

Tools like HerSafeSpace, Digital Grassroots, and Mozilla's Trustworthy AI movement are open to youth input!

### 5. Keep Learning, Keep Teaching

The digital world changes fast, so never stop learning.

- Follow pages that talk about digital rights and safety.
- Read, listen, attend webinars, join safe online forums.
- Pass it on. Everything you learn, teach someone else.

Because the strongest champions are students and teachers at the same time.

# Glossary of Terms

## **Block (on social media)**

A feature that stops someone from contacting you or seeing your posts.

## **Cyberbullying**

When someone uses the internet or phone to repeatedly send mean, hurtful, or threatening messages to another person.

## **Cyberstalking**

When someone keeps watching, messaging, or following you online in a way that makes you feel scared or unsafe.

## **Doxxing**

When someone shares your private information online (like your address or phone number) without your permission, to shame or harm you.

## **Digital Footprint**

The trail of information you leave behind when you use the internet — like posts, searches, photos, and comments. It's often permanent.

## **Digital Safety**

Protecting yourself online by using strong passwords, privacy settings, and reporting harmful behaviour.

## **End-to-End Encryption**

A security feature (used by apps like WhatsApp) that makes sure only you and the person you're chatting with can read your messages.

## **Gaslighting**

A form of manipulation where someone makes you question your memory, feelings, or reality. In OGBV, it's used to make victims feel like they're "overreacting" or imagining the abuse.

## **Gender-Based Violence (GBV)**

Any harmful act done to someone because of their gender — including sexual harassment, rape, emotional abuse, or control. Online forms are called OGBV.

## **Hashtag Activism**

Using hashtags like #EndRapeCulture or #StopOGBV to raise awareness, speak up, or start conversations on social media.

## **Impersonation**

When someone pretends to be you online by creating a fake profile or using your name or photos without permission.

## **Non-Consensual Image Sharing (NCII)**

When someone shares private or sexual photos/videos of you without your permission. Also called "revenge porn."

## **OGBV (Online Gender-Based Violence)**

Any kind of bullying, harassment, blackmail, or abuse that happens online — especially targeting women, girls, or marginalised groups.

## **Online Harassment**

Repeated and unwanted messages, threats, or insults sent over the internet to upset or scare someone.

## **Password Hygiene**

Using strong, unique passwords and changing them often to protect your online accounts.

## **Privacy Settings**

Tools on apps and platforms that let you control who sees your information, posts, and activity.

## **Report (on social media)**

Telling the platform (like Instagram or Facebook) that someone is breaking the rules by harassing or abusing you.

## **Revenge Porn**

A harmful act where someone shares private sexual images or videos of you without your consent, often to shame, punish, or control you. It's illegal in many countries.

## **Safe Space**

A place (online or offline) where you feel supported, respected, and free from harm or judgement.

## **Screenshot**

An image of what's on your screen. Often used to collect evidence of abuse.

## **Survivor**

Someone who has experienced abuse or violence and is still standing, healing, and growing. We use "survivor" instead of "victim" to show strength and dignity.

## **Trolling**

When someone intentionally posts rude or offensive comments online to upset people or cause arguments.

## **Two-Factor Authentication (2FA)**

An extra security step that asks for a code (often sent to your phone) after you enter your password, making it harder for hackers to get in.



# HerSafeSpace Digital Safety Manual



**Email:** brainbuilderedu@gmail.com **Tel:** 07068775529  
**Nigeria 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](http://www.thebrainbuilders.org)

[www.hersafespace-gbv.org](http://www.hersafespace-gbv.org)

 @BrainBuilders01

  BrainBuildersYouthDevelopmentInitiative