UN COVID-19 Response and Recovery Fund

#RecoverBetterTogether

A Guide for Women and Girls to Prevent and Respond to **Cyberviolence**

This guidance note has been produced by UN Women and UNICEF under the joint UN project 'Accelerating Women's Empowerment for Economic Resilience and Renewal: The post-COVID-19 reboot in Armenia', implemented by UNDP, UNIDO, UNICEF and UN Women. This joint project is possible thanks to the contributions to the UN Response and Recovery Fund by the governments of Netherlands, Denmark, Switzerland, Norway, Sweden, Republic of Korea, Finland, New Zealand, Croatia, Iceland, Thailand, Slovak Republic and Cambodia. Funded by the UN COVID-19 Response and Recovery Multi-Partner Trust Fund (UN COVID-19 MPTF), the project will advance priorities set out under the UN's COVID-19 Socio-economic Response and Recovery Plan for Armenia (SERRP).

Author(s): Amira Diallo
Editor(s): Faria Salman Asif, Nvard Manasyan and Jeffrey Stern
Designer(s): Asya Fatma Bağcı

November 2021

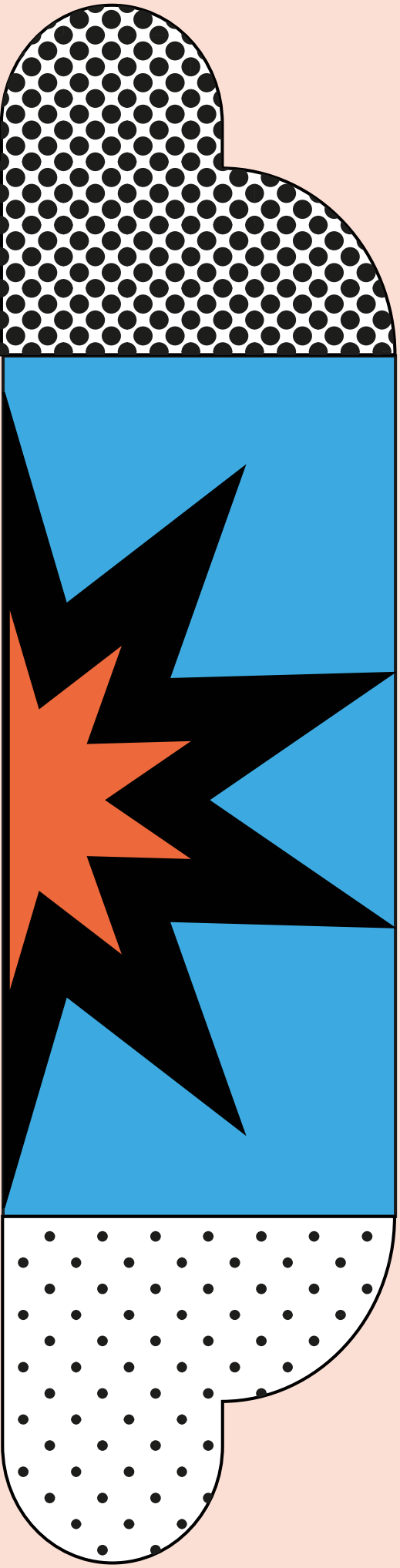
This guide was developed as part of

United Nations MPTF Office

A Guide for Women and Girls to Prevent and Respond to **Cyberviolence**

Restrictions, lockdowns and other response measures to the COVID-19 pandemic have boosted people's already-growing online presence, interactions and reliance on digital services. This connective technology holds enormous potential for empowering women and girls; it expands access to public services, creates opportunities for education and skills development, enables social engagement at a distance, provides a wealth of entertainment and open doors to employment and entrepreneurship. Unfortunately, it can also lead to cyberviolence — harms such as bullying, harassment, loss of privacy and direct violence — especially against women and girls who are just crossing the digital divide. These risks need to be eliminated so that women and girls have equal access to and use of digital tools and can equally benefit from growth in the digital economy.

This guide was created to help you build your knowledge of cyberviolence and will provide some essential practices and strategies to minimize being subjected to it — and to be able to respond in case it happens.



WHAT IS CYBERVIOLENCE?

Cyberviolence is when a person (or group of persons) uses an online-connected device to cause someone to suffer sexual, psychological, economic or any other form of harm, often by exploiting their target's circumstances, characteristics or vulnerabilities. Cyberviolence also includes actions that help to cause harm or merely threaten to cause harm. Though it takes place online, cyberviolence can often lead to direct physical harm. Though anyone can experience cyberviolence, women and girls are at greater risk, especially to severe harassment and sexualized abuse.

WHAT FORMS DOES CYBERVIOLENCE TAKE?

Cyberviolence takes many, often overlapping, forms. The most common types of cyberviolence include cyber-harassment; cyberbullying; revenge porn; cyberstalking; online child sexual exploitation, sexual abuse and child pornography; and sextortion.

Cyber harassment includes threats of physical or sexual violence; statements or defamatory falsehoods that embarrass their victim among family, friends and co-workers; unwanted sexually explicit emails or other messages; offensive advances on social media and other platforms; requests to send personal photos; and hate speech that targets someone based on factors such as their race, sex, ethnicity, religion, disability or sexual orientation. Cyber harassment often comes in a terrorizing 'storm of abuse' that combines several of these actions.

Cyberbullying is "an aggressive, intentional act or behaviour that is carried out by a group or an individual, using electronic forms of contact, repeatedly and over time against a victim who cannot easily defend him or herself."[15] "It can take place on social media, messaging platforms, gaming platforms and mobile phones. It is a repeated behaviour, aimed at scaring, angering, or shaming those who are targeted." Cyberbullying involves acts such as sending unwanted, hurtful or threatening messages; teasing or ridiculing; spreading rumours; making unpleasant comments; sharing pictures or video without consent; stealing an online identity and using it to hurt others; and deliberately ignoring someone or leaving them out of activities in order to hurt their feelings.

Revenge porn is "the online distribution of sexually graphic photographs or videos without the consent of the individual in the images."[17] Perpetrators are often ex-intimate partners who obtained the files during a relationship or are friends or acquaintances (and even strangers) who gained unauthorized access to the victim's private files. Reasons for distributing revenge porn include retaliating against someone for ending a relationship, publicly shaming and humiliating the victim, and basic cruelty (e.g. 'trolling'). Revenge porn can inflict substantial damage on the target's offline life, including creating rifts or ending relationships with the target's new partners, upending family ties, and getting targets fired from their job.

Cyberstalking is "stalking by means of email, text (or online) messages or the Internet. Stalking involves repeated incidents, which may or may not individually be innocuous acts, but combined, undermine the victim's sense of safety and cause distress, fear or alarm."

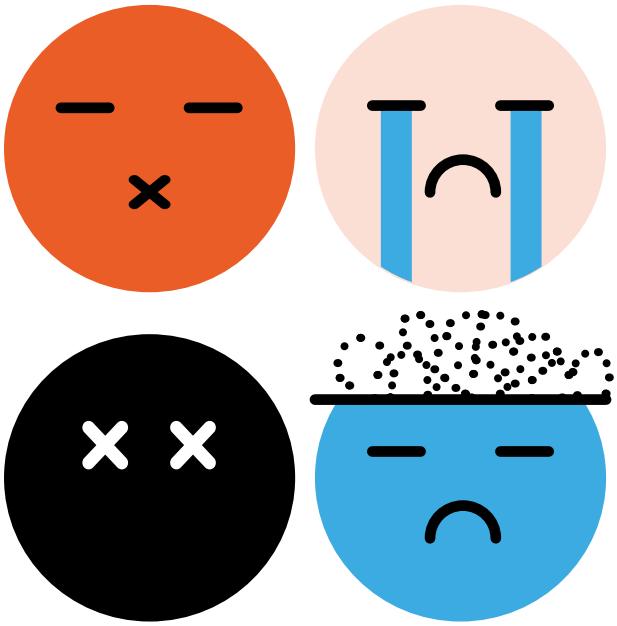
Online child sexual exploitation, sexual abuse and child pornography are major forms of cyberviolence that use online technologies to target children, often involving "the use of information and communication technology as a means to sexually abuse and/or sexually exploit children." Forms include soliciting children for sexual purposes, recruiting, or coercing a child into prostitution and pornography and live streaming of child sexual abuse. Child pornography is "the representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or representation of the sexual parts of a child for primarily sexual purposes," as well as the use of a child to create such a representation.

Sextortion is "a term in popular discourse that encompasses activities that (a) involve manipulation or coercion to perform sexual activities for the benefit of the perpetrator and/or to create sexually explicit images of the victim and (b) the traditional crime of extortion." Sextortion includes the threat to expose sexual images in order to make a person do something.

WHO COMMITS CYBERVIOLENCE?

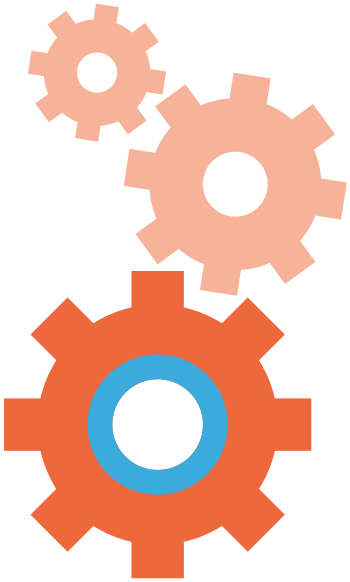
Cyberviolence can come from anyone — strangers met on- or offline, friends, colleagues or once- intimate partners. It can happen between peers and between different generations. Some perpetrators never reveal their identity, remaining anonymous by using a pseudonym. Cyberviolence often involves power imbalances between the victim/survivor and the perpetrator. Evidence has demonstrated that men and boys are the primary perpetrators of cyberviolence, particularly in the case of intimate partner stalking.

THE IMPACTS OF CYBERVIOLENCE

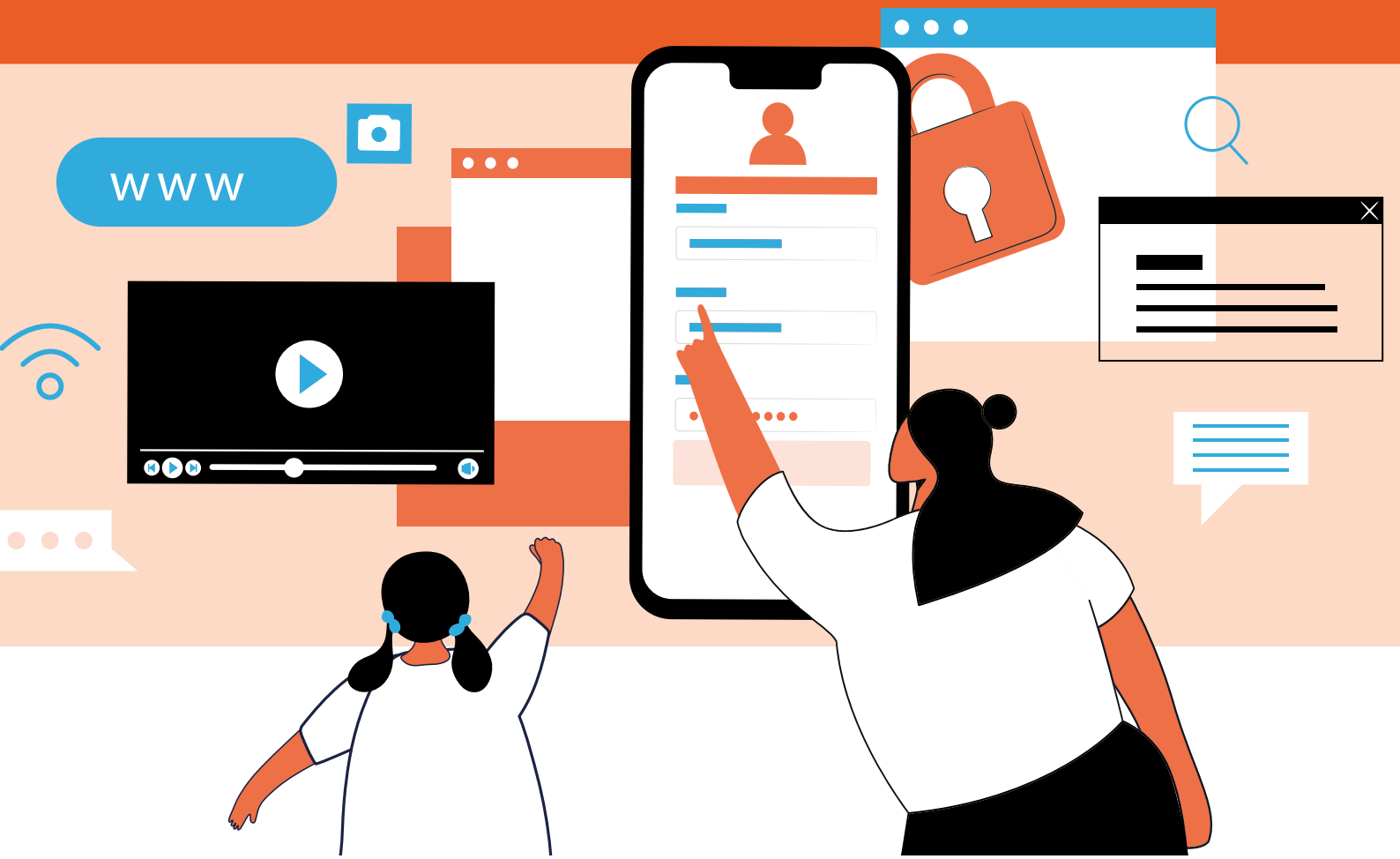


Although cyberviolence can affect anyone, women and girls are more vulnerable and experience different and more traumatic forms. The long-lasting effects of cyberviolence include a wide variety of behavioural, emotional, mental, physical and social impacts.

Behavioural impacts include quietness or, conversely, aggressiveness; poor school attendance; isolation or withdrawal from a group of people; and substance abuse or addiction. **Emotional impacts** can include feeling upset, embarrassed, stupid or angry and feelings of insecurity. **Mental impacts** often include anxiety and fear, lowered self-esteem, lack of trust in others, self-harm and suicidal thoughts, decreased interest in activities and a decline in academic or job performance. **Physical impacts** can include sleep disturbances, fatigue, changes in activity patterns or habits and increased depressive symptoms, including stomach aches and headaches. **Social impacts** can include being laugh at, a tarnished reputation, violations of intimacy, invasions of privacy, stigmatization and ostracization.



HELPFUL DOs AND DO NOTs FOR PREVENTING AND RESPONDING TO CYBERVIOLENCE



DOs

PREVENTING CYBERVIOLENCE

- **DO consider using a pseudonym instead of your real identity** as your personal email address or username, particularly if you feel uncomfortable when using online sites.
- **DO avoid using your professional email address** for personal Internet activities.
- **DO always set up your social media and online profiles yourself** so that you have control over the information you want to share.
- **DO consider with whom you share** your phones and other personal data.
- **DO make the best use of your devices' security settings,** following instructions to better protect yourself.
- **DO use security measures on all your digital devices,** such as antivirus software to protect against malicious programs (particularly keystroke loggers) and two-factor authentication to protect your login credentials (especially in common areas/hotspots and when granting third-party permissions to apps).
- **DO ensure your password is strong and kept secure.** Create strong passwords that are unique to each site, service and account and that are easy to remember so you don't have to write them down.
- **DO regularly change your passwords** to maximize your personal devices' security.
- **DO keep your software updated** in order to ensure that exploits and vulnerabilities are quickly patched.
- **DO transmit sensitive information only when connected to secure, known networks.** Even if a public network has a password, it is not necessarily secure. If possible, prioritize private networks (e.g. from your own devices, your family's or your workplace's network) over public networks.
- **DO be cautious and wary** of requests you receive online, particularly those asking for personal information. Even simple questions like "where do you live" or "where do you work" can reveal personal information that can be used to stalk or harass you.
- **DO make ample use of available security tools and settings.** Most social media apps and services allow you to block people who send you unwanted messages or comments — you can often block a person before it becomes harassment. You can also report problems to service providers or local authorities.
- **DO reset all your account passwords** (from your email and social media accounts to your bank accounts) **when separating from a relationship or partner,** especially if they are behaving in an abusive, worrisome, threatening or difficult manner.
- **DO regularly conduct Internet searches on your name** and check the sites where you appear online. If you find unauthorized information about yourself, immediately contact the site moderator to have it removed. Many services can be slow to respond; remain steadfast and persistent in your efforts until the content is taken down.
- **DO limit the information your devices share,** such as location or phone number. If you need to share information for business purposes, be sure to separate your personal information from your professional information.

DO NOTs

PREVENTING CYBERVIOLENCE

- **DO NOT share intimate pictures** with anyone online (even a trusted individual).
- **DO NOT share picture or video files of your friends and family without their consent;** you cannot control the way other people will use the files.
- **DO NOT share your or your friends' personal information** on public forums or chat servers.
- **DO NOT feel obligated to provide personal information** when filling in optional fields when registering with online sites (optional fields are typically not marked with an asterisk).
- **DO NOT give your passwords to anyone,** even persons you know.
- **DO NOT use personal information in your password** (such as birth date, name or nickname). Avoid frequently used passwords and never use the same password on more than one platform. Never record passwords in a written diary or computer file unless you can ensure their secure, encrypted (and password-protected) storage.
- **DO NOT attack or insult anyone while participating in discussion groups.** If you disagree with the person, state your position objectively and factually; being as polite online as you would be in person minimizes the occurrences of online retaliation.

DO

RESPONDING TO CYBERVIOLENCE

Remember: there is no reason for you to ever put up with any kind of cyberviolence

DO seek help from someone you trust; this is one of the most important first steps you can take.

- **For girls,** speak to a trusted adult that you feel safe talking to. It can be your parents, a close family member, another trusted adult or a school counsellor or a favourite teacher.
- **For women,** it can be your husband, a family member, your employer, a religious leader or a trusted friend.

DO clearly express dislike and ask the person to stop. If you do not express it explicitly, the perpetrator may believe that by not complaining, you are consenting.

DO prevent further communication from the perpetrator by blocking their email address, cell phone number and by deleting/blocking them from your social media contacts. Social media companies are obligated to keep their users safe and usually offer reporting links; look for links to formally report inappropriate behaviour.

DO save evidence. Keep abusive emails, text messages or screenshots of social media posts to show what took place when you seek support from services providers or the police.

DO distance yourself from phones, laptops and technology and spend time doing alternative activities with trusted friends and family. The more time you spend with activities that relax you, the less significance cyberviolence will have on your life. This will boost your self-esteem, increase your resilience and lessen the sense of being overwhelmed by the negative impacts of cyberviolence.

DO share your feelings. Expressing what you've experienced and what you're going through can make a huge difference in the way you feel, even if it doesn't change the situation. By speaking out about your experience, you may encourage others to report cyberviolence they are enduring.

DO seek help from a professional counsellor if you are not comfortable talking to someone you know. A professional is trained to effectively manage trauma and stress; trusted confidants are not necessarily sources of good advice.

DO contact the police if you feel unsafe or the abuse worsens. They may help protect you, open an investigation and may bring criminal charges against the perpetrator.

DO NOT

RESPONDING TO CYBERVIOLENCE

Remember: there is no reason for you to ever put up with any kind of cyberviolence

- **DO NOT blame yourself.** It is not your fault. No matter what a perpetrator says or does, you should not be ashamed of who you are or what you feel. The bully is the person with the problem, not you.

- **DO NOT let the situation get you down.** The perpetrator is often an unhappy, frustrated person who wants to have control over your feelings so that you feel as badly as they do. Do not give them the satisfaction.

- **DO NOT make a cyberviolence incident worse by dwelling on** it or reading related messages over and over. Instead, try to stop and instead focus on the positive experiences in your life. There are many wonderful things about you, so be proud of who you are.

- **DO NOT respond by email or text when you are angry or upset.** Wait until you are calm and composed to decide on what to do. You can decide to not respond or just respond to clearly express that you dislike the situation and request the person to stop. Sometimes a reaction is what the perpetrators are looking for because they think it gives them power over you. This can generate a chain of reactions that may be harmful to you. Do not engage in any question-and-answer scenarios that will make you feel uncomfortable.

- **DO NOT seek revenge.** Getting back at a perpetrator for retaliation will likely make the problem worse and could result in serious — and even legal — consequences for you.

For cyberviolence to stop, it needs to be identified, and reporting is key. Reporting can also help to show the perpetrators that their behaviour is unacceptable. If you do not report incidents, the perpetrator may continue and become more aggressive.

If you feel that you are in immediate danger, do not hesitate to contact the police

Take action if someone you know is being subjected to cyberviolence!

Share this guide with the person.

Listen and be supportive—your support can help the person to overcome the situation.

Do not blame or stigmatize the person.

You can help the person to think about practical solutions.

You can help the person to seek help with another trusted person, counsellor or authority.

Don't be a perpetrator of cyberviolence!

There are limits to freedom of expression with respect to others; it's imperative to respect the privacy of others in order to claim respect for one's own personal space.

The main elements of privacy — the boundaries that should be respected — include physical, sexual and civil identity, contact information, lifestyle, family, friends, romantic relationships, personal and religious beliefs, health and image.

You should consider privacy implications before you put anything on the Internet, and you should avoid publishing sensitive or sexually suggestive information or images of other people. Even if it is already posted online, you could still be contributing to cyberviolence.

Just because you are writing online or via a cell phone does not mean you can insult or threaten someone with impunity. Cyberviolence is legally punished in Armenia; you may be prosecuted.

You shouldn't do to others what you do not want to be done to you.

A MESSAGE FROM **UNICEF:**

Girls...

Talking to parents isn't easy for everyone. But there are things you can do to help the conversation. Choose a time to talk when you know you have their full attention. Explain how serious the problem is for you. Remember, they might not be as familiar with technology as you are, so you might need to help them to understand what's happening.

They might not have instant answers for you, but they are likely to want to help, and together you can find a solution. Two heads are always better than one! If you are still unsure about what to do, consider reaching out to other trusted persons (a close family member, a counsellor, the sports coach, your favourite teacher, etc.). There are often more people who care about you and are willing to help than you might think!

RESOURCES FOR HELP AND MORE INFORMATION

Resources available in Armenia

The Safe You mobile app provides information and awareness on gender-based violence for women and girls (including cyberviolence against women and girls). The app facilitates contact with police and support service organizations for support services.

Download the app at https://safeyou.space

The following organizations are Safe You services providers that provide support for cases of cyberviolence. You can directly reach out to them.

Women's Resource Centre
+374-77-991280
womenofarmenia@gmail.com
https://womenofarmenia.org

Women's Rights Centre
010 54 28 28
info@wrcorg.am
http://www.wrcorg.am/en

Sexual Assault Crisis Centre
0 800 01 280 / 077 99 12 80
sacc.arm@gmail.com
http://www.saccarmenia.org/

Other resources

Instagram:
- https://about.instagram.com/community/parents
- https://about.instagram.com/community/safety

Facebook:
- https://www.facebook.com/safety/bullying/teens
- https://www.facebook.com/help/?page=214189648617074

Twitter:
- https://help.twitter.com/en/using-twitter/blocking-and-unblocking-accounts
- https://help.twitter.com/en/safety-and-security/report-abusive-behavior

Websites offering information and awareness

Stompoutbullying.org is a website that spreads information and supports parents and young people to reduce and prevent cyberbullying, sexting and other forms of digital abuse. The organization deters violence in schools, online and in communities and educates against homophobia, LGBTQ discrimination, racism and hatred.

Webwise.ie offers advice and support for young people, teachers, youth workers and parents through information, advice and free education resources that address a range of Internet safety concerns.

A Guide for Women and Girls to Prevent and Respond to **Cyberviolence**

November 2021

UN COVID-19 Response and Recovery Fund

#RecoverBetterTogether