RESPONDING TO

ONLINE VIOLENCE

A PRACTITIONER'S GUIDE

This publication has been produced with financial support from Safe Online. However, the opinions, conclusions, and recommendations expressed herein are those of SEED and Online Violence Task Force and do not necessarily reflect those of Safe Online.

Table of Content

This guidance document was created by SEED, a non-governmental organization registered in the Kurdistan Region of Iraq, and Co-chair of the Online Violence Taskforce (OVTF), and reviewed and endorsed by its members. The OVTF is a national coordination platform established in 2021 and has the mandate to address the full spectrum of online violence in Iraq, including Technology-Facilitated Gender-Based Violence (TFGBV), Technology-Facilitated Child Sexual Exploitation and Abuse (TF-CSEA), cyberbullying, and digital harassment. The Task Force brings together UN agencies, NGOs, civil society, and government actors to strengthen coordination between GBV and Child Protection sectors, enhance prevention and response mechanisms, build capacity, promote survivor- and child-centered approaches, and advocate for stronger policies and systems to protect women, girls, and children across Iraq and the Kurdistan Region of Iraq.

Introduction

This resource serves as a guidance note to support case managers, frontline responders, and protection actors when addressing Online Violence (OV) cases in Iraq and the Kurdistan Region of Iraq. It is intended as a supplement to existing case management standard operating procedures (SOPs), providing additional considerations, tools, and approaches specific to cases of Technology-Facilitated Gender-Based Violence (TFGBV) and Technology-Facilitated Child Sexual Exploitation and Abuse (TF-CSEA). This guidance is designed to complement, not replace, existing organizational SOPs and should be applied within the standard GBV/CSEA case management process. It provides practical, survivor-centred and rights-based recommendations for responding to cases involving online violence, highlighting the specific considerations these cases require in relation to mental health and psychosocial support, safety and protection planning, digital risk and evidence management, and engagement with law enforcement and other service providers.

Technology-Facilitated Gender-Based Violence (TFGBV)

An act of violence perpetrated by one or more individuals that is committed, assisted, aggravated and amplified in part or fully by the use of information and communication technologies or digital media, against a person on the basis of their gender.[1]

Technology-Facilitated Child Sexual Exploitation and Abuse (TF-CSEA)

Refers to situations involving digital, internet and communication technologies at some point in the abuse or exploitation. "Technology-facilitated" and "online" are closely related but distinct terms used to describe forms of abuse and exploitation that can occur entirely online or through a mixture of online and face-to-face interactions between perpetrators and children. Online forms of abuse and exploitation generally refer to the production, dissemination, possession, etc. of child sexual abuse material, grooming of children for sexual purposes, live streaming of child sexual abuse, and sexual extortion of children.[2]

This guidance is designed to be used within case management processes that are grounded in the Age, Gender, and Diversity (AGD) approach. It underscores the need for responses to online violence to reflect the different risks, barriers, and service needs of survivors of all ages, genders, disabilities, and other diversity characteristics, and to ensure equitable, safe, and appropriate access to services.

Purpose

This document addresses the lack of specific online violence guidance for response actors in Iraq and Kurdistan by providing a dedicated resource that fills critical gaps in practical direction for handling Technology-Facilitated Gender-Based Violence (TFGBV) and Technology-Facilitated Child Sexual Exploitation and Abuse (TF-CSEA). It is designed to supplement, not replace, existing GBV and Child Protection case management standard operating procedures (SOPs) by by equipping practitioners with targeted guidance, tools, and knowledge to respond safely and effectively to online violence and to support more appropriate, coordinated, and survivor-centered outcomes for both adults and children. The document sets out key risks and considerations, recommended actions, and the roles of relevant service providers in addressing survivors' physical safety, mental health and psychosocial needs, legal options, and digital protection.

Note: The guidance is intended for use with both adults and child survivors. For child cases, child protection protocols must always be observed.

1 Making All Spaces Safe, UNFPA, 2021

2 Interagency Working Group on the Sexual Exploitation of Children. (2025, April). Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. Second Edition. ECPAT International: Bangkok

Types of Technology-Facilitated Gender-Based Violence

Cyberstalking

Use of technology to stalk and monitor someone's activities and behaviors in real-time or historically. It involves repeated unwanted monitoring, communication, or threats.[3]

Doxing

Disclosure of personal data online along with malicious suggestions for others to contact the person to cause more harm or with indecent intent.[4]

Hacking

Use of technology to gain illegal or unauthorized access to systems or resources for the purpose of acquiring personal information, altering or modifying information, or slandering and denigrating the survivor.[5]

Hate Speech

Any kind of communication in speech, writing or behavior, that attacks or uses pejorative or discriminatory language with reference to a person or a group on the basis of who they are, in other words, based on their religion, ethnicity, nationality, race, color, descent, gender or other identity factor.[6]

Image-Based Abuse (IBA)

Consists of using images to coerce, threaten, harass, objectify or abuse. One form of IBA is image-based sexual abuse (IBSA), which involves at least one of three behaviors: taking, sharing or threatening to share sexually explicit images without consent.[7]

Online Sexual Harassment

Any unwanted sexual behaviour via electronic means and can include unwanted sexual solicitation; unwanted requests to talk about sex; unwanted requests to do something sexual online or in person; receiving unwanted sexual messages and images; having sexual messages and images shared without permission; and revealing identifying and personal information about a person online.[8]

Sexual Extortion

An act of threatening to share information about an individual (including images or videos) to the public, their friends or family online, unless a demand is met.[9]

3 Making All Spaces Safe, UNFPA, 2021

4 Youth Guide to End Online Gender-Based Violence. UN WOMEN 2022

5 Making All Spaces Safe, UNFPA, 2021 Making all spaces safe

6 Id. at 17

7 Id. at 67

8 Id. at 13

9 Youth Guide to End Online Gender-Based Violence. UN WOMEN 2022

Types of Technology-Facilitated Child Sexual Exploitation and Abuse

Child Sexual Abuse Material (CSAM)

Visual material, and may include written or audio content, that depicts, describes or represents any person under 18 years of age: (a) Engaging in real or simulated sexual activity; (b) In the presence of a person engaging in any sexual activity; (c) Whose sexual parts are displayed for primarily sexual purposes; or (d) Subjected to torture or cruel, inhumane or degrading treatment or punishment and such material is sexual in nature.[10]

Online Grooming

The process of establishing/building a relationship with a child through the use of the Internet or other digital technologies to facilitate sexual contact with that person.[11]

Live-Streaming of Abuse

Refers to real-time child sexual abuse streamed online. This means the data are transmitted instantaneously to the viewer, who can watch and engage while the abuse is occurring. Importantly for the viewer, streaming leaves no trace on the device, because no file is downloaded; when the streaming is stopped the child sexual abuse material is gone, unless the offender deliberately records it.[12]

Self-Generated Content

Sexual material created by children themselves, which can be coerced or manipulated through online grooming or child sexual extortion.[13] Children should not be held criminally liable for producing images of themselves.[14]

Sexual Extortion

A form of blackmail where children are threatened with the release of private or sexual images unless they provide additional images, money, or engage in sexual activities.[15]

Deepfakes

Digital images and audio that are artificially altered or manipulated by Artificial Intelligence and/or deep learning to make someone appear to do or say something he or she did not actually do or say.[16]

10 UNGA. (2024, December). United Nations Convention against Cybercrime. Article 2-14.

11 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. Second Edition.

12 Id. at 86

13 Id. at 74

14 CRC Committee. (2019, September). Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography. CRC/C/156. Paragraph 67.

15 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. Second Edition.

16 Making All Spaces Safe, UNFPA, 2021

Context-Specific Risks and Considerations for TF-GBV and TF-CSEA

Case managers, frontline responders, and protection actors responding to cases of OV must ensure that identified issues and concerns of survivors are addressed systematically, while maintaining a survivor-centered and rights-based approach.

In Iraq, TF-GBV and TF-CSEA present distinct and often heightened risks compared to offline forms of violence. Harm can be continuous, rapidly amplified, and difficult to contain, as abusive content may be stored, shared, and recirculated indefinitely, and perpetrators can maintain contact, surveillance, or coercion from a distance. Survivors may experience severe and prolonged psychological distress, ongoing safety threats that span both digital and physical environments, and complex challenges related to privacy, evidence, and content removal. In cases involving child sexual abuse material (CSAM), the online distribution of images or videos is a strong indicator that sexual abuse of the child is occurring or has occurred in the offline environment, requiring an immediate child protection response.

In Iraq and the Kurdistan Region, these heightened risks are compounded by conservative social norms and the documented prevalence of "honor-based" violence. The exposure or perceived exposure of online abuse can place survivors - particularly women and girls - at risk of serious secondary harms from family or community members, including stigma, social exclusion, restrictions on movement or access to education and services, forced marriage, and physical violence, and murder. For children, these dynamics may also trigger punitive or protective responses that do not prioritize the child's best interests, increase the risk of family-based violence, or result in the withdrawal of the child from school, digital access, or essential services.

These factors create additional and time-sensitive demands on case management and require coordinated, highly confidential, and context-specific interventions that prioritize survivor safety, dignity, best interests of the child, and informed choice. These efforts are further complicated by gaps in the legislative framework, the absence of clearly mandated government entities responsible for protective case management or criminal investigation, and the lack of standardized government protocols for handling TF-GBV and TF-CSEA cases, which can increase the risk of unsafe disclosure, breaches of confidentiality, and responses that are not child- or survivor-centered.

The following key areas highlight the critical domains in which practitioners must apply enhanced attention, specialized knowledge, and adapted actions to ensure safe, survivor-centered, and effective responses to TF-GBV and TF-CSEA cases.

Key Areas of Response

Practitioners should apply enhanced attention to the distinct risks, ongoing exposure, and cross-sector coordination demands associated with TF-GBV and TF-CSEA across the following domains:

- **Mental Health and Psychosocial Support Services:** Addressing acute and prolonged emotional distress and trauma related to exposure and reputational harm, and the ongoing psychological impact of content recirculation/ exposure, loss of control over content, fear of discovery, and revictimization.

- **Physical and Digital Safety Planning:** Safeguarding survivors from online and offline threats by assessing and mitigating risks related to perpetrator contact, monitoring, retaliation, and potential family or community-based harm.

- **Digital Risk Management and Safe Removal of Harmful Content:** Strengthening survivor digital literacy; identifying and managing ongoing threats; supporting the safe documentation of digital evidence, where appropriate; and facilitating the reporting and removal of abusive content.

- **Engagement with Law Enforcement and Protective Services:** Supporting survivors to safely navigate interactions with law enforcement and other legal or protective actors while prioritizing confidentiality, survivor rights, the best interests of the child, and the prevention of secondary harm.

This guidance helps practitioners:

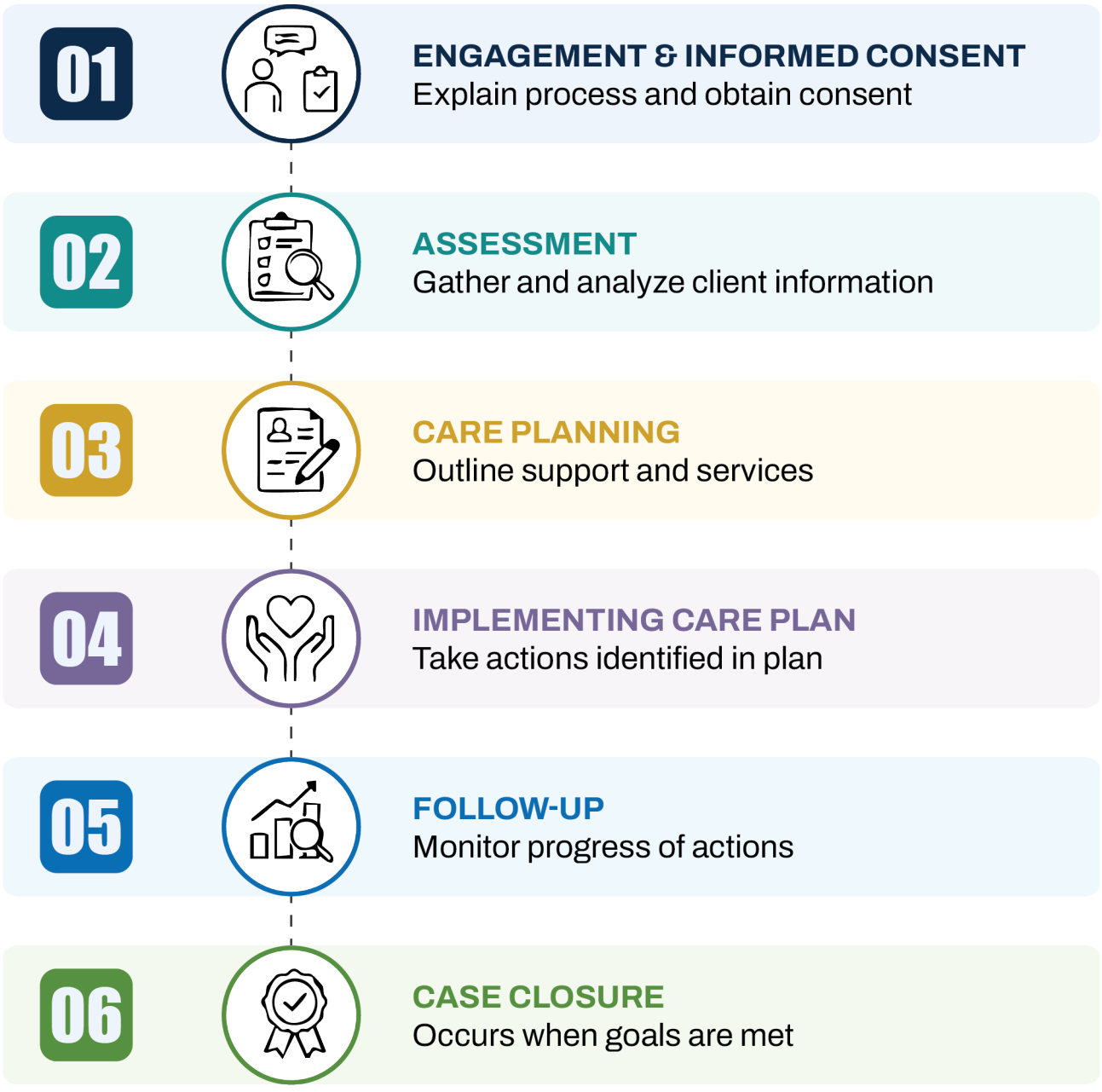
- Understand the Issue (ISSUE): Gain a clear understanding of the survivor's protection concerns and challenges.
- Identify Actions (ACTIONS): Identify appropriate steps for immediate and ongoing support.
- Utilize Tools (TOOLS): Access recommended resources and mechanisms appropriate for survivors.
- Coordinate with Actors (ACTORS): Identify and collaborate with appropriate organizations, service providers, and authorities.

Note! Cases involving children (under 18) should follow child protection and TF-CSEA protocols. Some TFGBV principles may be relevant but must be adapted to child-focused procedures.

Case Management Process

OV cases should be addressed through established, robust case management systems, and clearly defined referral pathways in line with standard operating procedures for GBV and Child Protection cases. These frameworks are critical to ensuring that survivors receive timely, quality, and well-coordinated support from appropriate service providers. Integrating OV services within existing GBV and violence against child (VAC) response structures strengthens continuity of care, promotes consistent application of survivor- and child-centered principles, and enables a comprehensive and effective response across all forms of violence.

Service providers and protection actors should assess, identify, and prioritize service needs: mental health and psychosocial services, health, legal, protection, digital safety, shelter, or child protection - and integrate these into the case plan. Service providers should facilitate safe and confidential referrals, supporting access to appropriate specialized and non-specialized services through informed consent, safe referral pathways, and coordinated follow-up. Special considerations follow.



Mental Health & Psychosocial Support Services (MHPSS)

ISSUE

Online Violence inflicts profound and prolonged harm to the mental, emotional, and social well-being of adult and child survivors. The ability of abusive content to be stored, recirculated, and repeatedly accessed can create a persistent sense of exposure, loss of control, and re-victimization. Survivors may experience anxiety, depression, post-traumatic stress disorder (PTSD), suicidal ideation, self-harm, and sleep disturbances and difficulty in daily functioning. These impacts are frequently compounded by fear of discovery, reputational harm, social stigma, and the risk of family or community retaliation. For children, the psychological effects may also include shame, self-blame, behavioral changes, withdrawal from school or social activities, and heightened dependency or distress linked to unsafe or punitive responses from caregivers.

Note: For cases involving children, all interventions must follow child protection case management protocols, apply best interests of the child principle, and ensure access to specialized, child-focused mental health and psychosocial support.

ACTIONS

Mental Health and Psychosocial Support (MHPSS) Interventions

Assess Survivor Safety and Immediate Risks: Evaluate the immediate safety concerns Including risks related to ongoing online exposure, perpetrator contact, family or community harm, and self-harm or suicide.

Provide Psychological First Aid (PFA): Deliver immediate, survivor-centered support to reduce acute emotional distress, reinforce coping strategies, and restore a sense of safety and control.

Assess Ongoing MHPSS Needs: Identify the nature and severity of psychological impacts, the survivor's existing support systems, and the need for specialized mental health care, and make referrals.

Ensure Urgent Referral for High-Risk Cases: Where there is imminent risk of self-harm, suicide, severe psychological deterioration, or immediate threats to safety, prioritize rapid referral to specialized mental health services in accordance with SOPs.

ACTORS

Contact the Online Violence Task Force, GBV Sector Coordination Group, or other Protection Coordination Groups and other coordination mechanisms to access the latest service mapping information, specialized MHPSS providers, and safe referral pathways.

Physical Safety/Protection

ISSUE

Due to conservative nature of society, TF-GBV and TF-CSEA cases carry a significant risk of violence not only from the perpetrator but also from family and community members. The non-consensual sharing - or threat of sharing - of private images, messages, or rumors can be perceived as bringing shame on the family, placing survivors, especially women and girls, at risk of blame, threats, physical harm, forced confinement, or honor-based violence from relatives or others in their community. As a result, online abuse can rapidly escalate into life-threatening offline harm.

These risks are often time-sensitive and require discreet, survivor-centered safety planning that prioritizes confidentiality and minimizes the possibility of unsafe disclosure. Safety concerns may also limit a survivor's freedom of movement, access to services, communication, education, or digital devices.

For children, the disclosure of online abuse may trigger punitive or protective responses that do not align with the best interests of the child and may increase the risk of family-based violence or withdrawal from school and essential services.

Note: For cases involving children, all safety planning and protection interventions should follow child protection protocols.

ACTIONS

To manage physical safety effectively, conduct comprehensive safety planning and risk assessment.

Assess Immediate and Imminent Risk: Determine whether the survivor is in immediate danger from the perpetrator, family, or community members and identify urgent protection needs.

Identify and Analyze Protection Risks: Assess the type, source, and likelihood of harm, including risks linked to:

- Family or community retaliation, including so-called "honor-based" violence
- Perpetrator contact, surveillance, blackmail, or extortion
- Public exposure or doxxing
- Financial coercion or exploitation
- Restrictions on movement, communication, education, or access to services

Determine Risk Level and Prioritize Actions: Classify risks by severity and urgency to inform immediate safety measures, referrals, and follow-up.

Identify Sources of Threat: Clarify who poses the risk (perpetrator, intimate partner, family member, community actor, online networks) to support targeted and realistic safety planning.

Develop and Implement a Survivor-Centered Safety Plan: Co-create practical, confidential strategies based on the survivor's context, choices, and available support systems. This may include safe shelter options, discreet communication methods, safe service access, and digital safety measures.

Activate Urgent Referrals for High-Risk Cases: Where there is a risk of serious or lethal violence, initiate immediate referral pathways in line with SOPs including to appropriate law enforcement entities including for shelter protection, if appropriate.

Assess Risk

1.) Financial Exploitation:
The use of the Internet and other forms of technology to exert financial pressure on a target.

2.) Physical Exploitation:
Any form of physical harm or threat to an individual's safety.

3.) Honor Based Violence Exposure: violence committed with the intention of restoring one's honor or the collective honor of the family, clan, or tribe.

4.) Public Harassment:
Non-consensual disclosure of personal information involving the public release of an individual's private, personal, sensitive information.

5.) Emotional Harm
Survivors may feel isolated, helpless, fear, shame, anxiety, depression, and unsupported—especially if their community blames them or minimizes their experience. In severe cases, trauma, self-harm, or suicide.

Assess Risk Levels

Assessing the severity of risks is crucial for prioritizing actions. Risks can be categorized as follows:

1.) High Risk:
Immediate and serious threat to the survivor's safety, including risk of physical violence, honor-based violence, suicide/self-harm, severe blackmail, or credible threats from the perpetrator, family, or community. Requires urgent action (within 24 hours) and immediate safety measures.

2.) Medium Risk:
Ongoing or escalating threats that may lead to harm if not addressed, such as continued harassment, online blackmail without immediate physical threat, increasing family pressure, or exposure of private content. Requires timely intervention and active safety planning (within 48 hours).

3.) Normal Risk:
Manageable level of risk where no immediate physical harm is identified, and threats are limited to online harassment or non-escalating harmful content. Requires monitoring, basic safety planning, and follow-up within standard case management timelines.

Identify Sources of Risk

Identifying the sources of risk is essential for developing targeted interventions. Risks can come from three different sources:

1.) Family:
Family members can either create risks, expand or mitigate risks.

2.) Perpetrator:
Individuals who engage in exploitative or abusive behaviors pose direct risks to survivor safety.

3.) Community:
Communities can create risks by accepting or ignoring harmful behavior, supporting abusers, or blaming or isolating survivors. This can include online shaming, spreading private information, or staying silent when abuse happens.

ACTORS

Contact the Online Violence Task Force, GBV Sector Coordination Group, or other protection coordination groups to access the latest service mapping information.

Digital Risk Management and Safe Removal of Harmful Content

ISSUE

Survivors of TFGBV and TF-CSEA often experience ongoing harm because abusive content can be repeatedly shared, accessed, and used for blackmail, coercion, or retaliation. The continued online availability of this material increases psychological distress and can heighten the risk of family or community violence. **Timely and safe removal of harmful content is therefore a critical protection need.**

Most survivors are unaware of available reporting and complaint mechanisms, do not know how to request content removal, or fear that taking action will escalate the abuse or lead to unsafe disclosure. Many also lack safe access to devices, private internet, or the digital literacy needed to protect their accounts and personal information. Digital safety interventions must therefore be integrated into case management in a survivor-centered, risk-informed, and confidential manner.

Without adequate knowledge, practitioners may unintentionally increase risk, fail to support survivors to preserve critical evidence, or overlook digital safety steps that are essential to preventing further harm. Technology-related interventions must therefore be integrated carefully into case management and safety planning processes.

Note: For cases involving children, support should follow child protection case management procedures, and use child-specific mechanisms for the handling and removal of sexual images or videos.

ACTIONS

All organizations that provide TFGBV and TF-CSEA case management should familiarize themselves with these tools and platforms and support survivors to take down or remove harmful content.

1. Conduct a Digital Risk Assessment

- Identify the type of online harm (e.g., sexual extortion, cyberstalking, deepfakes, impersonation).
- Assess whether the perpetrator has ongoing access to the survivor's accounts, devices, or location.
- Determine whether attempting content removal or reporting could escalate risk.
- Evaluate physical safety concerns before taking any digital action.

2. Support Survivors to Preserve Evidence (When Safe and Appropriate)

- Educate survivors on available reporting and response mechanisms i.e. platform based reporting mechanisms, dedicated reporting sites, or relevant legal processes.
- If a survivor decides to proceed with reporting or a legal case, and only with consent (assent and consent from a legal guardian in cases of minors), assess whether screenshots, links, usernames, timestamps, and URLs should be safely documented by the survivor, and provide guidance to do so.
- NGOs should not collect and store evidence, only in exceptional situations when information or materials are provided voluntarily and are critical to the safety and security of the survivor i.e. a child's legal guardian or family member is the perpetrator.
- Support survivors with instructions on how to proceed with their preferred reporting or response mechanism. NGOs should not submit or proceed on behalf of the survivor.
- Do not preserve or store illegal child sexual abuse material; follow child protection procedures.

3. Develop a Case-Specific Digital Safety Plan

- Based on risk level and survivor consent, support the survivor to:
- Change passwords and enable two-factor authentication.
- Review and strengthen privacy settings on social media and messaging platforms.

- Check devices for unknown applications or tracking features.
- Disable location sharing where necessary.

Limit contact or block the perpetrator if safe to do so.

4. Support Survivors to Remove or Report Harmful Content (With Informed Consent)

- Discuss risks and benefits of reporting content.
- Use appropriate platform reporting mechanisms or trusted reporting partners where available.
  - ◊ For adult survivors of non-consensual intimate image abuse, consider tools such as StopNCII.
  - ◊ For cases involving children, use child-specific reporting mechanisms such as Take It Down, in line with child protection protocols.
- Ensure the survivor understands possible outcomes, including delays or retaliation.

5. Refer to Specialized Actors When Required

- Where technical complexity exceeds case manager capacity, refer to trusted digital safety organizations or specialized cybercrime units.
- Coordinate with protection actors to ensure digital actions do not undermine physical safety planning.

6. Ensure Survivor Choice and Confidentiality

- All digital actions must be based on informed consent.
- Survivors should understand potential outcomes, including possible retaliation or delays in removal.
- Maintain strict confidentiality throughout the process.

Note: Digital safety measures should not replace broader protection planning but must be integrated into mental health support, physical safety planning, and legal response pathways to ensure a comprehensive and coordinated response.

TOOLS

These entities work across all platforms to report and remove online harmful contents. Practitioners should be familiar with when and how to use them as part of case management and safety planning.

StopNCII and Take It Down are both free tools designed to prevent the further spread of sexual images online by creating a secure digital fingerprint that helps participating platforms detect and block content before it is re-uploaded. Both work across major social media platforms and prioritize survivor privacy. Practitioners should select the tool based on the survivor's age and ensure that child protection protocols are followed in cases involving children.
StopNCII is intended for adult survivors (18+)
Take It Down, operated by the National Center for Missing & Exploited Children (NCMEC), is specifically designed for children and youth under 18 and is linked to child protection mechanisms.

INSM and Tech4Peace (T4P) are trusted reporting partners operating in Iraq that help escalate cases of online violence directly to major platforms such as Facebook, Instagram, TikTok, and Google. Unlike StopNCII and Take It Down, which focus primarily on preventing the redistribution of sexual images, INSM and T4P handle a broader range of online harms, including harassment, blackmail, impersonation, and harmful content. They are particularly useful when rapid escalation is needed, when content appears across multiple platforms, or when standard platform reporting has not resulted in timely action.

StopNCII is a free tool designed to support survivors (over 18 years old) of Non-Consensual Intimate Image (NCII) abuse. They support creating a digital footprint (hash) of an image or video to ensure it does not get posted again.

Contact details: https://stopncii.org/
How to report:
Step 1: Go to stopncii.org
Step 2: Click on "Create Your Case"
Step 3: Answer questions asked
Step 4: Select the photo/video from your device that you would like to protect.
Step 5: StopNCII will generate a digital footprint which prevents the photo being shared on social media
Step 6: It is vital to keep a record of your case number and unique pin so you can keep track of your case and follow up on it

Take It Down is a free tool designed to support children and youth who are survivors of sexual images or videos being shared online. It helps remove content and prevent further sharing, in coordination with child protection mechanisms. Take It Down is a service provided by the National Center for Missing & Exploited Children.

Contact details: https://takeitdown.ncmec.org/
How to report:
Step 1: Go to https://takeitdown.ncmec.org/
Step 2: Click on "Get Started"
Step 3: Answer questions asked
Step 4: Upload the image/video or provide the link where it is located
Step 5: Take It Down will initiate the removal process and provide follow-up guidance
Step 6: Keep a record of your case ID and follow any instructions from child protection services

INSM is a trusted platform in Iraq for reporting online violence. They have established trusted partnerships with platforms like Facebook, TikTok, and Instagram, which allows them to respond more quickly to harmful content.

Contact: WhatsApp: +964 783 588 2244 or email: report@insm-iq.org
How to report:
Step 1: Whatsapp message or email Digital Emergency HelpDesk
Step 2: Provide details and evidence (screenshots, links, etc.)
Step 3: Submit the report

Tech4Peace (T4P) is a safe and confidential platform for reporting about online violence incidents in Iraq and the Kurdistan Region and is a trusted partner with Tiktok, Facebook, Google, and Instagram, meaning that they get quicker service when they refer cases.

Online link: https://t4p.co/
How to report:
Step 1: Download the Tech4Peace app on your app store
Step 2: Click the cog in the top right corner of your screen to pick which language you want the app in
Step 3: Click the image button in the bottom center of the page
Step 4: Click the option "Report Form"
Step 5: Pick the best option pertaining to what you want to report.
Step 6: Follow the instructions till submitting the report

Note: to backup your evidence Tech4Peace may ask for screenshots to support your case.

ACTORS

Major platforms such as Facebook, Instagram, Snapchat, TikTok, WhatsApp, and X (Twitter) have built-in reporting and blocking tools that allow users to flag harmful content, harassment, threats, or image abuse directly within the app. These mechanisms are often the first step to request content removal or limit contact with the perpetrator. Practitioners may support survivors in using these tools when it is safe to do so, ensuring evidence is preserved and risks of retaliation are assessed beforehand.

Facebook

Step 1: Go to the post you would like to report
Step 2: Click the three dots next to the post
Step 3: Click report post
Step 4: From the options given pick the one that best describes your problem

Instagram

Step 1: Click the three dots on the top right corner of a post
Step 2: Click report
Step 3: Choose why you are reporting the post
Step 4: Decide whether you want to block or restrain the account you are reporting

Snapchat

Step 1: Click the three dots on the top or bottom right corner of a post
Step 2: Click report this snap
Step 3: Choose why you want to report
Step 4: Add a comment to back your report

TikTok

Step 1: Go to the video you would like to report
Step 2: Press the share button
Step 3: Press the report button that looks like a flag
Step 4: Select why you are reporting
Step 5: Send your report

Whatsapp

Step 1: Open the chat of the sender you want to report
Step 2: Tap the contact name or number and open chat info
Step 3: Scroll down to the bottom and press report
Step 4: Press report or block and report

X (Twitter)

Step 1: Click the three dots on the top right corner of the post
Step 2: Click report this post
Step 3: Choose why you are reporting the post
Step 4: Answer the questions with the given options
Step 5: Decide whether you want to block or mute the account you are reporting

Law Enforcement and Protection Services

ISSUE

While law enforcement agencies in Iraq and the KRI have responded to incidents of online violence, there is no comprehensive legal framework specifically criminalizing all forms of OV, no single mandated investigative body, and no standardized protocols governing case handling. Cases are therefore pursued under existing legislation, which can create procedural gaps, inconsistent practices, and risks related to confidentiality and survivor safety.

Survivors should be clearly informed of their right to report, the role and limitations of law enforcement in responding to such cases, available reporting pathways, possible legal outcomes, and the potential risks associated with filing a complaint. The primary functions of law enforcement are to investigate reported offenses, take measures to stop ongoing crime, collect and preserve evidence, and initiate criminal proceedings. In some cases, law enforcement may provide protective orders or access to protective shelter.

ACTIONS

Support survivors to safely navigate interactions with law enforcement in a survivor-centered, risk-informed, and confidential manner, ensuring that legal action does not expose them to additional harm and is integrated into the broader case management and legal response. Survivors must understand the available reporting pathways, possible legal outcomes, and any risks associated with filing a complaint.

Conduct a Legal Risk–Benefit Assessment

Before supporting a survivor to file a complaint:

- Identify the appropriate law enforcement for reporting. (See list below)
- Assess immediate and secondary risks (including retaliation from perpetrator, family, or community).
- Determine whether reporting could escalate physical harm or honor-based violence.
- Evaluate the survivor's protection needs before, during, and after reporting.
- For child survivors, follow child protection reporting procedures and protocols.

Ensure Informed Consent (Adult Survivors)

- Clearly explain the survivor's right to report and the option not to report.
- Explain possible outcomes (investigation process, court procedures, possible confrontation with perpetrator, timeline).
- Clarify potential risks including potential lack of confidentiality, family notification, community awareness, delays in proceedings.
- Confirm voluntary and informed decision-making before proceeding.

Note: For cases involving children, reporting must follow child protection and best interest procedures.

Support Survivors to Preserve and Prepare Evidence Before Reporting

- Support safe documentation of digital evidence (screenshots, URLs, usernames, timestamps).
- Ensure evidence is preserved before survivors attempt content removal, where appropriate.
- Coordinate with cybercrime units when necessary to avoid compromising investigations.
- Maintain confidentiality and secure case file management.

Prepare the Survivor for the Reporting Process

- Explain where and how the complaint will be filed.
- Clarify what information may be required.
- Discuss the possibility of interviews or follow-up questioning.
- Offer accompaniment where possible and appropriate.

- Inform survivors that investigations may take time.
- Clarify that digital crimes, especially cross-border cases, may present legal or jurisdictional limitations.
- Avoid guaranteeing specific outcomes.

Integrate Safety Planning Before and After Reporting

- Develop a protection plan in case the perpetrator is notified or becomes aware of the complaint.
- Assess the need for shelter, relocation, or emergency protection measures.
- Plan follow-up support if family or community backlash occurs.

Continue Psychosocial and Protection Support Throughout the Process

- Provide ongoing emotional support during investigation.
- Monitor evolving risks.
- Maintain regular follow-up and adjust safety planning as needed.

ACTORS

The decision regarding which law enforcement agency to approach depends on the organization's established coordination pathways or working relationship with a particular agency, while ensuring the case type aligns with that agency's mandate. Strong professional relationships can support safer and more efficient referrals. Practitioners should accompany the survivor through the reporting process. In cases involving children, practitioners should always accompany the child when reporting to law enforcement and ensure that child protection protocols are strictly followed to safeguard the child's safety, dignity, and well-being throughout the process.

Hotline Phone Numbers

Iraq	
South and Center Governorates of Iraq	911
National Regular Police Hotline (Request for Assistance and Protection)	104
Community police hotline (Assistance in cases of domestic violence)	497
Directorate of Family and Child Protection (to report the harassment against women and adolescent girls and cases of torture)	139
National Security Office hotline (report electronic extortion)	131

The Kurdistan Region	
Directorate of Combating Violence Against Women and Families (DCVAW)	119
Police	104 / +964 750 808 8080
The Kurdistan Region Security Service (Asayish) - Erbil	066106 / +964 750 252 2728
The Kurdistan Region Security Service (Asayish) - Sulaimani	+964 770 390 6223

SEED

www.seedkurdistan.org

@SEEDKurdistan

Safe Online


Iraq Task Force
Online
Violence
فريق عمل العراق – العنف الإلكتروني
گرووپی کاری عێراق- تووندوتیژی ئەلیکترۆنی