InjusticeWatch

ONLINE VIOLENCE GUIDE

Introduction

Online abuse is one of the most significant threats faced by journalists today, especially women, people of color, and LGBTQ+ people. Journalists are regularly targeted in harassment designed to intimidate, shame, and silence them for their work. According to the International Center for Journalists, 73% of women journalists have experienced online abuse ranging from personal insults posted online to online threats of real-world violence. And 20% of women journalists have experienced offline harassment or attacks that stemmed from online abuse. The cumulative effects of ongoing online harassment can lead to burnout and drive journalists out of the profession. In extreme cases, targeted online attacks can lead to physical threats and danger.

In 2023, Injustice Watch joined the International Women's Media Foundation's (IWMF) Digital Safety Cohort to help the organization learn best practices for proactively protecting our staff from online abuse, develop policies for responding to online harassment when it occurs, and train our team on these policies and digital safety tools.

This guide and our new policies will be incorporated into our employee handbook. Copies of this guide are also available on the shared Google Drive.

Defining online abuse

PEN America defines online abuse as the "pervasive or severe targeting of an individual or group online through harmful behavior."[1]

- **Pervasive** because, while some individual incidents of online abuse, such as insults or spam, may not rise to the level of abuse, a steady drumbeat of incidents, or a coordinated onslaught, does.
- **Severe** because even a single incident of online abuse, such as a death threat or the publishing of a home address, can have serious consequences.
- **Online** includes email, social media platforms (such as Twitter, Facebook, Instagram, and TikTok), messaging apps (such as Facebook Messenger and WhatsApp), blogging platforms (such as Medium, Tumblr, and WordPress), and comments sections (on digital media, personal blogs, YouTube pages, and Amazon book reviews).

Injustice Watch recognizes that online abuse is a serious problem and that it can never be completely prevented or avoided. This guide is intended to provide Injustice Watch staff with tools to proactively protect themselves as best as possible from online abuse and personal data breaches and to provide guidance on what to do if online abuse occurs.

[1] For a complete glossary of terms related to online abuse and harassment, see https://onlineharassmentfieldmanual.pen.org/defining-online-harassment-a-glossary-of-terms/.

How Injustice Watch is managing online abuse

Working with IWMF, Injustice Watch has created a set of policies and tools for helping employees protect themselves against online abuse. We will host an annual digital safety meeting, during which we will review best practices for digital safety and provide technical support for setting up digital safety tools. Supervisors are encouraged to check in with employees on a regular basis about any digital safety concerns or online harassment.

Digital safety

One of the best ways to protect yourself from online abuse is protecting your personal data and securing your online accounts. Injustice Watch strongly encourages all staff members, but especially those on editorial, to take steps to remove your personal information from the internet and to protect your personal and work accounts as best as possible. IWMF will be providing us with additional training on digital safety tips and tools.

Protecting your personal data

Follow this checklist to secure your personal information and accounts. Key steps to take are below:

- Look through your social media accounts and delete photos or posts that identify where you live, provide full names of family members, or include your personal email address or phone number.
- Set your social media accounts to private.
- Use this list to identify popular online data brokers and how to remove your information from their lists.
- If you feel your personal data is particularly vulnerable, consider using part of your professional development fund to purchase a subscription to DeleteMe, which is a service that removes your personal data from online data brokers on an ongoing basis.

Use this Online Violence Risk Assessment to determine your personal vulnerability to online abuse — which may change depending on your beat, what stories you're working on, and your past exposure to online harassment.

Account security

Use a password manager

All Injustice Watch staff members are required to use 1Password to create unique, strong passwords for all work accounts. For 1Password to be effective, you **must** create a strong master password that is never used for any other site. (Click here for tips on creating a strong master password, which should be memorable to you but hard to crack.) Print out your 1Password Emergency Kit, write your master password on it, and store the physical copy in a safe place. Then, use 1Password to generate strong, unique passwords for every account.

Injustice Watch staff members are also strongly encouraged to use 1Password or another password manager for your personal accounts. 1Password offers free family accounts for journalists.

Set up two-factor authentication

Two-factor authentication requires you to receive a one-time passcode — usually via text, email, or a third-party authentication app — to sign in. This helps protect your accounts even if your username and password are hacked. Injustice Watch requires all employees to set up two-factor authentication (2FA) on all workplace accounts, including your Injustice Watch email, Wordpress, Slack, and other tools. We also recommend that you use 2FA for all your non-workplace accounts — especially accounts that could be used to find your personal information, including email, social media accounts, bank/financial accounts, etc.

Reporting and escalation policy

If you are the target of online abuse or harassment, you should report it immediately to your **direct supervisor** and the **operations manager**. The "Reporting and Escalation Policy" below outlines the process that Injustice Watch will take in response to online abuse.

Key steps include:

- Report any online abuse or harassment that feels concerning to you. Nothing is too small to report.
- Document messages you receive. If reading or documenting them is triggering or stressful, you can provide account access to the operations manager or another trusted staff member to document for you.
- The operations manager will inform the leadership team and ensure the staff member is supported through any organizational response.
- If the abuse involves a threat of violence or physical danger, the executive director will contact legal assistance and law enforcement, with the employee's permission.

Resources

- Online Violence Response Hub
- PEN America Online Harassment Field Manual
- Pen America/IWMF "Digital Safety Snacks"

This guide was created with the support of the International Women's Media Foundation, as part of their 2023 News Safety Cohort.

INTERNATIONAL WOMEN'S MEDIA FOUNDATION

InjusticeWatch

ONLINE ABUSE REPORTING AND ESCALATION POLICY

This policy outlines how to document, report, and escalate instances of online abuse and harassment, and how Injustice Watch will respond to online threats against its employees. Injustice Watch takes all threats seriously and the physical and online safety of our employees is of utmost importance. Online threats should be immediately reported through the process outlined below.

This guide and our new policies will be incorporated into our employee handbook. Copies of this guide are also available on the shared Google Drive.

When to report an online attack

Whenever an online attack raises your concern level, it should be documented and reported to **your direct supervisor** and the **operations manager**.

Examples of the types of abuse that should be reported include:

- Messages that include threats of physical or sexual violence
- Threats made against your family members
- Private or personal details — particularly location information — published about you, another staffer, or someone you have interviewed
- Your address, phone number, or email address being circulated with a threat to do harm (doxxing)
- Coordinated attacks or messages from multiple accounts or a targeted smear campaign
- Any other message that raises your concern level. **There doesn't need to be a specific reason — if it feels concerning to you, report it.**

Documenting online abuse

Take screenshots of any threatening or concerning messages on social media, and save copies of threatening emails. If the abuse is repeated and ongoing, create a log of messages you've received, including the date and time, platform/medium, and nature of the attack.

If you've responded to any of the messages, be sure to include screenshots of your responses, too. Though you may regret having said certain things, a failure to document all aspects of your harassment could end up harming you if you ever end up in court. You don't have to prove you've reacted perfectly at every step in order to pursue your harasser.[2]

If documenting and re-reading the harassment or abuse feels triggering or overwhelming, you can provide your account information to the **operations manager** or another trusted colleague and ask them to document the abuse.

[2] More guidance on how to document online abuse is available at https://onlineharassmentfieldmanual.pen.org/documenting-online-harassment/

Reporting online abuse

The **operations manager** will inform **editorial leadership,** the **director of development and operations,** and the **executive director,** and coordinate support for the impacted staffer. The leadership team will seek to understand the situation, identify areas where the staffer needs assistance, and coordinate communication so that the staff member can focus on safety.

What happens next

Responses to any online attack will be taken quickly, yet thoughtfully. Responses will vary greatly depending on the nature of the attack but will focus on supporting the safety and well-being of the affected staff member and other staff.

The **operations manager** will monitor both the organization's and the affected staffer's social media accounts for additional threats. If necessary, the affected staff member may choose to turn over access to their social media accounts to the **operations manager** for closer monitoring.

The **director of development and operations** and the affected staff member's direct supervisor will coordinate with the **executive director** about whether to respond to the attack from the organization's social media accounts. Responses could include a statement of support for the impacted staffer.

The **operations manager** will notify other newsroom staff of the situation, if this could help prevent further escalation of the attack and does not cause additional harm.

The **executive director** will contact law enforcement, if necessary, and only with the consent of the affected staff member. Law enforcement will be contacted if there is a threat of physical danger to the staffer. It is also a crime if the harasser uses language that is lewd, obscene, or profane with intent to harass, intimidate, torment or embarrass.

The **executive director**, in consultation with the board of directors, legal counsel, and the leadership team, will determine additional steps necessary for the safety of the staffer and the rest of the Injustice Watch team. This could include relocation of the staffer, protection via law enforcement or security officers, consultation with security experts, consultation with counseling experts, temporary closing of the Injustice Watch office, and other steps as necessary. Depending on the scale of the attack, the **executive director** will handle any requests from other news organizations.

This guide was created with the support of the International Women's Media Foundation, as part of their 2023 News Safety Cohort.

InjusticeWatch

CHECKLIST FOR PROTECTING YOUR DATA

With journalists facing increasing online harassment and attacks, reviewing, managing and securing your online data is an essential step to increasing your security. The data you have online can be used by people to target you. Removing personal information, such as photos of your family, your home address or date of birth, is a good way to better protect yourself. Use the following checklist to help manage your online data. You can learn more about how to take these steps in PEN America/IWMF's "Digital Safety Snacks" video series (some of which are also linked below).

Look yourself up online using all search engines

- Use incognito mode or a private window function to carry out the search
- Review images and video as well as news
- Review your social media and look through photos, comments and old posts
- Note down any data you would like to remove

Remove data from the internet

- Remove or make content private on your social media accounts
- Remove personal content from sites that you own, such as a personal website
- Ask family, friends, and colleagues to remove content with your information from their sites or social media accounts
- Check internet archive services, such as the Wayback Machine, and ask them to remove content
- Consider requesting Google Maps/Apple Maps to blur out your house
- Ask Google Search to remove unwanted data from its search engine
- Contact owners of websites or public databases to see if they will/are able to remove data about you. This list provides common online data brokers and instructions for requesting that they remove your data.
- If you feel your personal data is particularly vulnerable, consider purchasing a subscription to DeleteMe, which is a service that removes your personal data from online data brokers on an ongoing basis. Injustice Watch employees may use their PD funds for this purpose.

Secure your accounts

- Turn on two-factor authentication for all your accounts
- Use a password manager and create long passwords of more than 16 characters
- Learn more about securing your accounts here.

Other

- Set up Google Alerts for your name, address and date of birth
- Create calendar reminders to review your online profile regularly — how frequently depends on your risk, but at least once every 3-6 months.

InjusticeWatch

ONLINE VIOLENCE RISK ASSESSMENT

This risk assessment document will guide you through a series of questions designed to keep you safer online. By the end of the assessment, you should have a clearer idea of how to better protect you and your online data. Please include details on how you will reduce risk.

This risk assessment should be used alongside the **IW Checklist for Protecting Data**. The risk assessment and checklist can be completed by both journalists and editors in the newsroom. It should be reviewed in advance of publication of each story published by Injustice Watch.

Online violence and your story/beat

Have you previously been targeted online? If so, please note down who you feel was behind the attacks.

Is the subject of this story likely to cause a backlash online? Have you previously been targeted for covering this type of story?

Research and make a note below of the groups of people who are likely to target you online as a result of this story.

Are the people or groups of people you listed above known to target journalists online? If so, what types of attacks do they carry out? For example, manipulating photos of journalists, publishing the personal details of journalists online or harassing a journalist's family members.

Are you contacting sources via your social media accounts for this story? If so, have you taken steps to secure your data and accounts?

Is there a threat of physical violence? For example, do the people who are threatening you online — or might in the future — live nearby?

Based on the answers you wrote down above, below are some of the steps you might want to take to protect yourself from online threats. This can also be done using the Checklist for Protecting your Personal Data.

Review and remove your online data

Is your address publicly available online? If so, what steps can you take to have it removed?

Have you looked up your name using all search engines and made a note of all content you are unhappy having online? Note any content you want removed below.

Have you reviewed photos and videos available about you online, including content stored in your social media accounts? Note any photos or videos that you want removed below.

Have you reviewed old social media posts for content that could be used to potentially discredit you?

Have you reviewed what data is available online with regards to your close family, including partners, children, parents and siblings? Note any content you want removed below.

Have you spoken with family, friends and colleagues about what data can and can't be shared about you online?

Newsroom support

Have you spoken with your editor(s) about any concerns you may have regarding online abuse and a particular story? Note down your concern below.

Do you know who to contact should you receive a serious online threat? Do you know who to contact if your accounts are hacked? If not, review the IW Online Abuse Reporting and Escalation Policy.

Have you and your editor discussed a plan for if you receive targeted online abuse as a result of your work?

This document was created with the support of the International Women's Media Foundation, as part of their 2023 News Safety Cohort.