The Seattle Times

Online Abuse Guidelines

Created in 2021 by Naomi Ishisaka, Danny Gawlowski, Ela Stapley and Harlo Holmes
in a collaboration between The Seattle Times and IWMF.

Online abuse is one of the largest threats that U.S. journalists now face. Journalists, particularly women and journalists of color, are regularly targeted in harassment designed to intimidate, shame and silence. 73% of women journalists have experienced online abuse ranging from personal insults posted online to online threats of real-world violence. 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.

Journalists should be prepared for a range of possible online abuse. Peer support and mental health counseling can help cope with a range of personal insults posted online. Digital security steps should be taken to help prevent hacking and impersonation. Monitoring or scrubbing your personal information online can help prevent doxxing, swatting or other forms of online incitement of physical violence. Knowledge of other common types of online abuse can help you recognize tactics and respond more quickly.

PEN America defines online abuse as the pervasive or severe targeting of an individual or group online through harmful behavior:

- **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.
- **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.
- **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).

The Seattle Times newsroom leadership recognizes the reality of online abuse. These guidelines are meant to help reinforce awareness, strengthen peer support groups, encourage staff to secure their online privacy and help us react quickly to online attacks.

Reducing harm from online harassment

Online harassment can be ongoing and multi-faceted. Support for our journalists to counter the cumulative effects of this harassment also needs to be ongoing and multi-faceted. This includes:

INTERNATIONAL WOMEN'S MEDIA FOUNDATION

These online harassment policies and procedures were created with support from the International Women's Media Foundation.

- Trainings will be held to help offer support techniques. These trainings will be recorded and posted, then included in onboarding documents for new employees.
- Within the Newsroom Mentorship program, mentors will be encouraged to discuss online harassment with their mentees.
- Newsroom supervisors will be encouraged to take time within team meetings as well as within individual meetings to check in with staffers' experiences with online harassment.
- Time will be made within a newsroom staff meeting each year to discuss online harassment.
- Once we return to the office, we will create a physical place to post some of the most egregious messages that staffers receive. Staffers can choose to post harassment they received and can choose to read the posted examples.

The goal of the group conversations will be to help depersonalize personal attacks. It's important to remember that these attacks, which are often made to be very personal, are part of a larger effort to silence journalists. In sharing examples, staffers are encouraged to see the common trends among these attacks and see that the target is the message more than individual journalists as messengers. Staff are also encouraged to share coping techniques, with the recognition that different techniques work differently for each person.

Within our own commenting systems we have greater control over online harassment. The Seattle Times has taken steps to promote civil discussions, including:

- Creating a Commenting Code of Conduct to discourage personal attacks and violations of privacy and other unacceptable behavior.
- Using Coral as our commenting system, which automatically scans all comments for "toxicity" and banned terms. These filters not only flag problematic comments but also provide feedback to commenters, promoting more civil behavior.
- Ongoing moderation of comments and banning of problem users.
- Limiting comments to subscribers, which has drastically reduced the overall number of toxic comments.

Security and privacy steps to take before an online attack

In addition to online harassment, journalists have been targeted by more severe online attacks. Specific reporting, such as the coverage of extremist groups, increase the likelihood of an online attack. There are several steps every staffer should take now to increase their online security and privacy.

- Set up two-factor authentication for key online accounts where possible. This security step is required for all major Seattle Times systems. Consider setting this up for your key personal services as well, such as personal email and social media accounts.
- Set up unique, complex passwords for each of your online accounts. Consider using a password service, such as 1Password, that can generate and track unique passwords. 1Password offers free services for journalists.
- Review your online footprint and take steps to remove personal data that you don't want in the public domain.

These online harassment policies and procedures were created with support from the International Women's Media Foundation.

- Be prepared by anticipating likely online harassment. Different stories will attract different levels of trolling and different types of attack. It is a good idea to complete a risk assessment highlighting any concerns beforehand. Flag any possible attacks with management before publishing.
- If you are reporting on a subject or group that increases your risk of doxxing (a type of targeted online attack that involves the publishing of private information), discuss with your editor and an AME the possibility of using an online privacy service such as DeleteMe or PrivacyDuck. However, these services can be expensive and only effective in limited circumstances. The newsroom usage of these services will be limited only to credible, specific threats.
- Familiarize yourself with the Seattle Times online abuse training and reporting site.

Reporting, responding and escalating during an online attack

Whenever an online attack is out of the ordinary or raises your concern level, it should be documented and reported to your departmental editor. If any of the following are true, document and report the incident:

- Private or personal details, particularly location information, are published about you, another staffer or someone you have interviewed.
- Messages include threats of death, violence or in-person harassment.
- Multiple social accounts join a coordinated attack.
- Something about the message raises your concern level.

When this happens, make a screenshot of the message and any relevant posts. Note the URLs of any published posts. Inform your department editor, then upload the screenshots via the Online Abuse Reporting form.

As the incident is escalated, the following people will take on these roles:

- The department editor will inform the AME group while coordinating support with the impacted staffer. The department editor will seek to understand the situation, identify areas where the staffer needs assistance and coordinate communication so that the staffer can focus on safety.
- The AME group will coordinate with HR. HR will coordinate with law enforcement, if necessary. 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. In situations where there is no threat of violence, HR will still contact the police upon request. In those circumstances, the police are more likely to follow up if there is a way to identify the harasser such as a phone number, a name, or a traceable email address involved.
- The AME group will coordinate with the Digital Editor and producers to monitor social media or other platforms. If necessary, a producer can be made available to assist with responses from the impacted staffer's personal social media accounts, so that the staffer can focus on safety concerns.

These online harassment policies and procedures were created with support from the International Women's Media Foundation.

- The AME group will coordinate with Marketing for a response to the attack from any main social accounts, if this is decided to likely cause more help than harm. Responses could include a statement of support for the impacted staffer. Depending on the scale of the attack, the Marketing team will also handle any requests from other news organizations.
- The AME group 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 AME group, in consultation with the department editor and HR, will determine additional steps necessary for the safety of the staffer. This could include relocation of the staffer, protection via law enforcement or security officers, consultation with security experts, consultation with counseling experts and other steps as necessary.

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 Seattle Times staff.