Best Practices For News Organizations:

How to Protect and Support Journalists Harassed Online

PEN AMERICA

Coalition Against Online Violence

Contents

Introduction

What Is This Guide and Who Is It For?

This guide offers **best practices for the leaders, managers, and editors of news organizations who are committed to protecting and supporting their staff and freelancers in the face of online abuse**. These best practices were distilled over two years by a team of experts from civil society organizations, media organizations, and professional associations.

Threats, doxing, impersonation, cyber mobs, and other abusive tactics are a growing problem in the journalism industry. Reporters are caught in an increasingly untenable double bind. They have to be online to do their jobs, yet their visibility and the very nature of their work make them lightning rods, especially if they belong to groups disproportionately targeted for their identity and/or if they cover politicized beats. Harassment strains the mental and physical health of its targets and can lead to stress, anxiety, fear, and depression. In extreme cases, it can escalate to physical violence.

Because of these risks, online abuse has forced journalists to self-censor, step away from online platforms, or leave their jobs altogether—directly undermining efforts to cultivate diverse and equitable news organizations. And while abusive tactics can appear personal, they are often deployed as part of a broader, concerted effort to suppress a free and independent press. **By better protecting their staff and freelancers, news organizations can defend press freedom in the face of government, corporate, and individual efforts at intimidation and censorship.**

Who Developed This Guide?

Best Practices for News Organizations: How to Protect and Support Journalists Harassed Online was developed by the Newsroom Working Group of the Coalition Against Online Violence (CAOV), a network of 90+ global organizations working to find better solutions for women journalists facing online abuse.

PEN America, as lead of the Newsroom Working Group, spearheaded this guide in close collaboration with ACOS Alliance, International Press Institute, WAN-IRFA, 100 Days in Appalachia, Women's Media Center, Susan McGregor of Columbia University's Data Science Institute, Canadian Association of Journalists, Freedom of the Press Foundation, Women in Journalism, Vita Activa, Stop Online Violence Against Women, and ARIJ. This project was co-led by Viktorya Vilk, Director of Digital Safety and Free Expression at PEN America and Jeje Mohamed, Holistic Safety and Security Advisor and former Senior Manager of Digital Safety and Free Expression at PEN America.

This guide builds on the work of over a dozen press freedom and civil society organizations, which have developed invaluable resources for how newsrooms can support their staff and freelancers in the face of online abuse (which we highlight throughout this guide). Multiple newsroom leaders and staff offered extensive input on this guide.

We are deeply thankful to all of the individuals and organizations who contributed their time and energy to creating this guide, including many of the industry leaders and experts who belong to the CAOV. We want to particularly express our appreciation to the IWMF for founding the CAOV and to Craig Newmark Philanthropies for supporting the CAOV and this guide.

Coalition Against Online Violence

International Press Institute 75

Media Freedom

The Canadian Association of Journalists
L'Association Canadienne des Journalistes

100 Days in Appalachia

INTERNATIONAL WOMEN'S MEDIA FOUNDATION

Craig Newmark Philanthropies

How Do I Use This Guide?

We understand that guidance for news organization leaders cannot be one-size-fits-all. A news organization's size, location, regional focus, capacity, audience, and finances will determine whether and how to adopt any best practices. We also understand that grappling with the issue of online abuse, let alone tackling a comprehensive guide of best practices, can feel overwhelming.

We encourage you to think of this guide as a menu of best practices to choose from and adapt—rooted in your own knowledge of your news organization and your team(s)—rather than as a checklist of to dos. You do not need to implement these best practices in any specific order, or all at once, but rather can experiment with them in any order and at various levels and build on them over time.

The guide is divided into two main sections:

- **Best Practices for Organizational Leaders:** These are the leaders who make decisions on organization-wide priorities, policies, finances, etc.
- **Best Practices for Managers and Editors:** These are the leaders who directly supervise staff and freelancers.

Within each section are distinct best practices, each subdivided into:

- **What**
- **Why**
- **How**
- **Cost and Organizational Size**
- **Resources and Examples**

A dollar sign rating offers estimated costs as per the key below:

$ = free or low cost, but may require modest staff time

$$ = requires staff time and financial investment

$$$ = requires considerable staff time and financial investment

While putting some of these best practices in place may require a significant investment of time and resources, we can assure you that bolstering your organization's capacity to navigate online harassment will ultimately save you time, money, and stress, help you hire and retain more diverse talent, and strengthen your reporting.

Where Do I Start If I'm In Leadership?

News organizations of **all sizes** can start with the following best practices (in any order):

- Raise Awareness and Shift Culture
- Develop Policies and Protocols
- Bolster Digital Security

If you lead a **small to mid-sized news organization**, here are some additional steps you can take:

- Assess the Scope
- Provide Training and Build Capacity for Staff & Freelancers
- Foster a Supportive Environment
- Issue a Statement of Support

If you lead a **mid to larger-sized news organization**, here are some additional steps you can take:

- Develop Reporting Channels
- Create A Task Force
- Provide Training and Build Capacity for Managers and Editors
- Educate Staff & Freelancers on Allyship
- Moderate Content

What Should I Do If I'm A Supervisor?

1. Reach Out and Listen
2. Assess Risk and Response
3. Document and Delegate
4. Communicate Policies, Protocols, and Resources
5. Seek Internal and External Support

Best Practices

For Organizational Leaders

1. Raise Awareness and Shift the Culture

What:

Make clear to staff and freelancers—through regular communication, written commitments, and action—that organizational leadership recognizes the seriousness of online abuse and expects managers, editors, and colleagues to do the same.

Why:

It is crucial for organizational leaders to create an environment where staff and freelancers who experience abuse feel safe and supported enough to ask for help.

How:

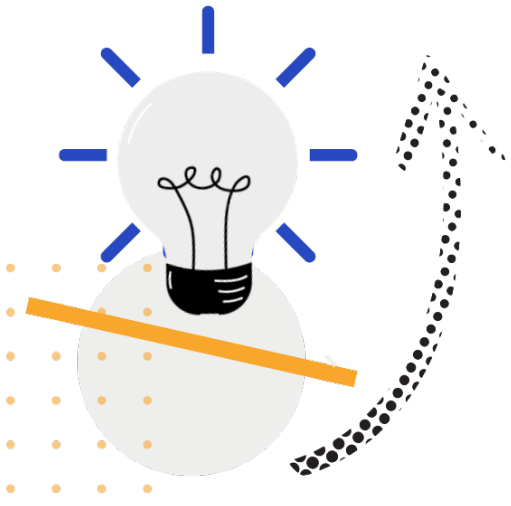
- **Communicate** this commitment explicitly in all-staff meetings and emails, team meetings, one-on-one check-ins, and organizational channels like Slack.
- **Demonstrate** this commitment by developing policies and protocols that address online abuse.
- **Reinforce** this commitment by consistently providing robust, sensitive support to staff and freelancers when they face abuse.
- **Prioritize** targeted individuals' experiences and needs over arbitration of what counts as abuse.
- **Acknowledge** that women, people of color, LGBTQ+ individuals, people with disabilities, and members of religious and ethnic minorities are disproportionately targeted for their identity and may need additional support.

Cost & Organizational Size $

Costs for **staff time**. Critical and cost-effective for **organizations of any size**.

Resources and Examples:

- The Seattle Times' article about dealing with targeted online abuse against their staff
- AP's public acknowledgment of the need to better address online abuse
- Australian Broadcasting Corporation's guidelines on preparing for exposure to larger audiences
- IWMF's Raising Awareness of Online Violence in the Newsroom (pp. 8-12)
- Women's Media Center's What Online Harassment tells us about our newsrooms: From individuals to institutions



2. Assess the Scope

What:

Assess the scope, scale, and impact of online abuse within your organization.

Why:

To most effectively address online abuse, it is essential to understand: how often staff and freelancers experience it; on which platforms they experience it; what kinds of tactics they experience; emotional, psychological, and professional impact; how identity and subject area affect the frequency and severity of abuse; and what actions targeted individuals have taken.

How:

- **Organize** a town hall or another moderated forum for group discussion of safety and online abuse and ensure that staff and freelancers are not penalized for showing vulnerability. This can help normalize conversations about online abuse while highlighting organizational resources.
- **Create** an anonymous survey and distribute it to staff and freelancers, ideally annually. Keep the survey concise and structured. Rather than collecting sensitive or traumatic details, consider providing an optional space for additional information, including about identity or specific experiences. Be transparent about who can access survey responses, how results will be shared, and how management will use the results. Maintaining confidentiality is critical. Note: the smaller the organization, the harder it is to ensure anonymity. To boost trust and participation, consider working with an external third party.

Cost & Organizational Size $ - $$

Costs for **staff time, consultancy fees, and/or survey software**. Feasible for **organizations of any size**. The most cost-effective options are a moderated group conversation or simple in-house survey. A more comprehensive annual survey, potentially run by an independent third party, requires a bigger investment.

Resources and Examples:

- IWMF's concise survey template, with a case study from the Anchorage Daily News (see page 17)
- IPI's survey template
- PEN America's detailed sample survey

3. Create a Task Force

What:

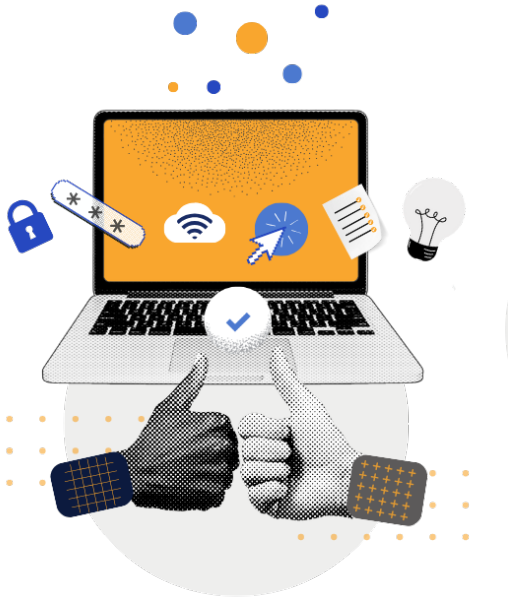
Bring together an internal task force of people with diverse backgrounds, experiences, areas of expertise, and skills to holistically address online abuse.

Why:

Different abusive tactics require different kinds of expertise to provide physical, digital, psychological, and/or legal support. Providing such support can also be time-consuming and emotionally demanding for a single individual, while a task force can share responsibilities and crowdsource skills.

How:

- **Develop** policies and protocols, work on their implementation, and advise on responses to instances of abuse as needed.
- **Include** representatives from various departments (such as senior leadership, physical security, digital security, IT, human resources, social media, audience engagement, editorial, reporters, legal, and diversity and inclusion).
- **Designate** a leader or champion to steer the group and serve as a point of contact for staff and freelancers.
- **Integrate** with existing safety teams or initiatives whenever possible.
- **Make** the task force diverse and inclusive, incorporating individuals who may be underrepresented in leadership positions.
- **Ensure** that anyone on the task force who has personally faced harassment is participating willingly.
- **Solicit** input, build trust, and secure buy-in among staff and freelancers.
- **Recognize** the efforts of task force members through financial compensation, recognition, or other means.



Cost & Organizational Size $ - $$$

Costs for staff time and/or consultancy fees. A task force is more practical for **mid-sized to larger organizations** with multiple departments and external experts.

Resources and Examples:

- IPI's actors involved and its job description of an online safety expert
- The Seattle Times' article about creating online abuse guidelines

4. Develop Policies and Protocols

What:

Create a **policy**—an organization's strategy for addressing online abuse experienced by staff and freelancers, including the resources and services offered, digital security requirements, expectations for professional social media use, and roles and responsibilities for navigating incidents. Include a **protocol**—which outlines the concrete steps that staff and freelancers can take to prepare for and respond to online abuse, including whom to ask for help and how.

Why:

Many news organizations lack policies or protocols to help journalists prepare for or respond to abuse. Social media policies often omit abuse, focusing instead on governing journalists' online activity. Clear protocols and policies, including proactive guidance on digital safety (particularly personal data and the secure use of social media/digital accounts), can foster a sense of safety and empowerment and minimize harm.

How:

- **Create** living documents that are regularly updated (ideally with time stamps) and referenced by leadership.
- **Ensure** that all policies and protocols are sensitive to race, gender, sexuality, and disability, given that online abuse disproportionately impacts people of color, women, LGBTQ+ individuals, disabled people, and members of religious and ethnic minorities.
- **Offer** a broad package of resources, training, and other services that address safety and online abuse. (See "Provide Training and Build Capacity for Staff & Freelancers," and "Bolster Digital Security")
- **Collect** all safety resources in a centralized, accessible place, potentially within an organizational intranet or staff handbook. (See "Communicate Policies, Protocols, and Resources.")
- **Distribute** safety policies to staff and freelancers digitally and physically, integrate them into onboarding documents, and post them on channels such as Slack.
- **Enlist** managers, HR, IT, and audience engagement teams to reinforce these policies and protocols.

Cost & Organizational Size $ - $$

Costs for **staff time and/or consultancy fees**. A news **organization of any size** can benefit from developing policies and protocols, which can vary in length, detail, and complexity; these do not have to be comprehensive from the outset and can evolve over time.

Resources and Examples:

- IWMF's templates for Online Violence Guide for the Newsroom and Reporting and Escalation Policy
- IPI's Protocol for Newsrooms to Support Journalists Targeted with Online Harassment
- The Seattle Times' Online Abuse Guidelines and article about creating guidelines
- The New York Times' social media guidelines
- Defector Media's digital harassment policy. (Please note: paywalled article)
- PEN America's Protocol for Online Abuse (published in Slate) and Best Practices for Employers
- Organizations such as PEN America, IWMF, and IPI work with media organizations to help them develop policies and protocols

5. Develop Reporting Channels

What:

Develop internal channels through which staff and freelancers can privately report online abuse or other safety concerns and request support.

Why:

Clear reporting channels make it easier for staff and freelancers to notify the organization once safety problems arise. They also improve employers' ability to assess threats and identify patterns of abuse across the organization (for example, multiple staff dealing with the same stalker).

How:

- **Offer** at least two channels for reporting, formally and informally (e.g., manager, HR, and/or a formal reporting mechanism). Make these channels easy for staff and freelancers to access and use, taking into account that they might be hesitant to speak to their manager directly.
- **Consider** carefully who should receive reports, what their specific responsibilities are, and the best ways to collect and distribute reports.
- **Monitor** the reporting mechanism regularly and ensure prompt follow-up with resources and support.
- **Develop** clear instructions for how and when to access these channels, including clarity about confidentiality practices, when to expect a response (including during non-work hours), and what support is available.
- **Ensure** that instructions for how to use the organization's reporting channels are a mandatory part of the onboarding process for staff members, freelancers, and leadership.
- **Consider** formalizing support for online abuse as a key component of the duties of relevant managers and HR personnel.
- **Communicate** reporting channels and resources through managers, editors, peer support networks, and corporate communications. (See "Communicate Policies, Protocols, and Resources.")
- **Ensure** that data collection and storage are secure, private, and confidential through data retention and deletion policies. Collect only information that is absolutely necessary. Be transparent about how and where the report will be stored and who will have access to it.
- **Implement** trauma-informed reporting practices that respect confidentiality, obtain consent, set clear expectations about issues like anonymity, and ensure that targets of abuse do not have to repeatedly recount their painful experiences.

Cost & Organizational Size $ - $$

Costs for **staff time, consultancy fees, and/or software**. Although reporting channels can vary in terms of mechanism and number of people involved, setting up multiple formal channels is more practical for **mid-sized and larger organizations**.

Resources and Examples:

- IWMF's template for Reporting and Escalation Policy and case study from Protocol Media (page 35)
- IPI's Newsrooms structures and support mechanisms / Reporting Systems

6. Provide Training and Build Capacity for Staff & Freelancers

What:

Empower staff and freelancers with guidance on how they can protect themselves proactively, respond to online abuse, and support others.

Why:

Most journalists rely on digital tools (email, messaging, search engines, social media), but few receive adequate training on using them safely and professionally. Digital safety can feel daunting, especially across multiple platforms. By offering practical and interactive training, workshops, and information sessions, news organizations can equip staff and freelancers with skills to protect themselves.

How:

- **Offer** holistic safety training (covering digital security, online abuse defense, risk assessment, processing trauma, and bystander intervention) to management, editors, reporters, photojournalists, finance and administration teams, communications specialists, interns, and support staff.
- **Provide** workshops for managers and editors on how to discuss online abuse and trauma and how to support staff who face abuse (see "Provide Training and Build Capacity for Managers and Editors").
- **Develop** this training in-house or with external support of civil society organizations

Cost & Organizational Size $ - $$$

Costs for **staff time and/or consultancy fees**. **All news organizations** can benefit from information sharing and training. One low-cost way to start is organizing a tips and skills exchange among your own staff and freelancers. While training can vary in cost and time commitment, many civil society organizations offer free or low-cost options.

Resources and Examples:

- IWMF's case study of Radio Free Europe (page 11), Online Violence Courses and Resources and guide to Better Protection for Freelancers Facing Online Violence
- PEN America, the Online News Association, and IWMF's Digital Safety Snacks
- Coalition Against Online Violence maintains a list of organizations that provide training, including PEN America, IWMF, IPI, CPJ, ACOS Alliance, and Freedom of the Press Foundation

7. Bolster Digital Security

What:

Be proactive about defending against online abuse by bolstering the organization's digital security, while also supporting individual staff and freelancers in reducing their online footprint and securing their accounts.

Why:

Bolstering both organizational and individual digital security empowers staff and freelancers, helps mitigate online abuse, and reduces harm—particularly from tactics such as doxing, hacking, phishing, and impersonation as well as from surveillance and intimidation by state actors.

How:

- **Start** with the basics. If your organization has IT or tech support staff or consultants, ensure that they are involved throughout.
- **Provide** organization-wide access to a password manager.
- **Require** all staff and freelancers to use a password manager and two-factor authentication on their professional accounts. Encourage them to do the same for their personal accounts.
- **Subsidize** a data scrubber service and organizational VPN.
- **Offer** hands-on digital safety training.

Cost & Organizational Size $$ - $$$

Costs for **staff time, consultancy fees, and/or software(s)**. Facilitating basic digital security hygiene is inexpensive and effective for **all organizations**, though changing individuals' behavior can be time-consuming. While password managers can be moderately expensive at the organizational level, some companies offer free or low-cost options. A comprehensive audit or revamp of organizational digital security practices is more costly, requiring in-house or external IT or cybersecurity expertise; however, civil society organizations offer subsidized support to under-resourced news organizations.

Resources and Examples:

- FPF's Training Program and Online Account Security guide
- IWMF's Checklist for Protecting Staff Data
- CPJ's Digital Safety Kit
- CyberPeace Builders' pro bono digital security support for nonprofits
- PEN America, Online News Association, and IWMF's Digital Safety Snacks
- PEN America's guidance on Protecting Accounts and Devices from Hacking and Managing Your Online Footprint and Protecting from Doxing
- OpenNews's Field Guide to Security Training in the Newsroom
- Global Cyber Alliance's Cybersecurity Toolkit for Mission-Based Organizations and for Journalists
- Consumer Reports' Security Planner
- Ford Foundation's Cybersecurity Assessment Tool

8. Foster a Supportive Environment

What:

Set aside time and resources to encourage staff and freelancers to create spaces where they can exchange ideas about shared challenges, including navigating online abuse and safety.

Why:

Online abuse is often profoundly isolating. Its targets may not have personal relationships with people who can relate to their experience, yet research shows that strong social connections can substantially reduce psychological harm. Giving staff and freelancers a safe space to share experiences and exchange practical tips with peers fosters well-being and resilience.

How:

- **Ensure** that staff and freelancers have adequate space, resources, and time during working hours to form peer support groups focused on online abuse and digital safety.
- **Give** peer support groups access to leadership, with confidentiality as needed so they can advocate for organizational change.
- **Clarify** that peers are not licensed psychologists or counselors and that the news organization's role is simply to facilitate support spaces and share resources. A consent form may be helpful to confirm that participants understand they are not receiving clinical care.
- **Consider** issues of encryption, data retention, and privacy and confidentiality settings if your organization is facilitating peer support through digital platforms.

Cost & Organizational Size $ - $$$

Costs for staff time and/or consultancy fees. While well-resourced news organizations might have the means to bring in licensed professionals, **all organizations** can facilitate open dialogue and foster spaces for staff and freelancers to discuss online abuse and mental health.

Resources and Examples:

- Reuters's and BBC's peer support networks, outlined here by the IPI
- Canadian Association of Journalists' Peer Support Program
- IWMF's Mental Health Guide for Journalists Facing Online Violence
- Vita Activa's peer support and psychological aid for journalists
- PEN America's The Power of Peer Support, a report outlining the benefits of peer support for journalists facing abuse

9. Moderate Comments

What:

Moderate public comments, including on news articles, blogs, and social media channels run by news organizations.

Why:

Abuse and disinformation can stifle debate and undermine targeted reporters and news organizations. Moderating comments from the outset can foster robust discussions and help mitigate the long-term impacts of abuse.

How:

- **Create** a code of conduct for organization-run platforms that solicit public or reader commentary. Clearly define what content is considered abusive.
- **Place** this code of conduct in a clearly visible spot close to where the commentary is solicited.
- **Enforce** this code of conduct as rigorously as possible.
- **Consider** removing comment features or allowing them only on select articles if your news organization lacks the resources to moderate all public commentary.

Cost & Organizational Size $ - $$

Costs for **staff time, consultancy fees, and/or comment moderation software**. Moderating content is more practical for **mid-sized to larger organizations**. While creating comment moderation policies or codes of conduct is lower cost, investing in personnel time or in software to help actively moderate comments is higher cost.

Resources and Examples:

- The 19th News' Community Guidelines
- The Wall Street Journal's community rules and FAQs
- BBC Sports' stance against social media trolls, which includes policies for blocking and reporting abusive comments
- World Association of News Publishers' Emerging Best Practices for Online Comment Moderation
- Coral's guide to writing a code of conduct and how to host/manage comment sections effectively
- Free or low-cost software such as Perspective or Coral can assist with proactively identifying and filtering harassment at scale

10. Issue a Statement of Support

What:

Consider issuing a public-facing or internal statement of support for staff and freelancers who experience severe online abuse—in close consultation with targeted individuals.

Why:

The power dynamics between a lone target and an abusive, often coordinated mob are extraordinarily uneven. An institutional statement signals support and care—to the targeted individual, the individual's colleagues, and potentially the public. A statement can alleviate the isolation, intimidation, and silence that the abuse is meant to induce. That said, a public-facing statement can also draw more attention to the abusive incident, so it's important to weigh the benefits and risks in consultation with the targeted individual.

How:

- **Balance** the needs and preferences of the targeted individual with those of the organization when deciding whether to issue a public-facing or an internal statement of support.
- **Ensure** that the targeted individual knows about and is comfortable with the statement.
- **Clarify** in advance the circumstances that warrant a statement of support.
- **Prepare** a template in advance that can be adapted to fit specific situations, ensuring that the template's language conforms to organizational policies and protocols.
- **Use** the statement to fact-check false claims, highlight the targeted individual's work (rather than the abuse), or call out the abuser's motives (which may include intimidation, silencing marginalized voices, undermining trust, suppressing a free press, and manipulating audiences).
- **Take** the opportunity to provide guidance, especially internally, on how others can safely and effectively support the targeted individual.

Cost & Organizational Size

Costs for **staff time and/or consultancy fees. Organizations of any size** can issue public or internal statements of support.

Resources and Examples:

- IWMF's What to Consider When Making Statements of Support (page 38) and template for a statement of support
- NBC's statement on attacks against Brandy Zadrozny
- The Verge's statement on attacks against Sarah Jeong
- Los Angeles Times' statement on retaliatory investigation aimed at Alene Tchekmedyian
- North Atlantic Books' statement on attacks against Thenmozhi Soundararajan
- Journalist Glenn Cook's op-ed in defense of a colleague at the Las Vegas Review Journal
- IPI's Protocol for Newsrooms to Support Journalists Targeted with Online Harassment
- PEN America's Best Practices for Employers
- Australian Broadcasting Corporation's statement on abusive comments toward female journalists and statement on racist attacks against ABC staff

11. Provide Training and Build Capacity for Managers and Editors

What:

Provide training and build capacity for managers and editors on how to identify, respond to, and support staff and freelancers facing online abuse.

Why:

Staff and freelancers should feel that their safety and well-being is taken into account as part of decision-making on editorial value and reputation. Responses to traumatic events need to be intentional and human-centered rather than ad hoc in order to build trust and resilience.

How:

- **Prepare** managers and editors for their roles by providing training on how to regularly check in on well-being, support a colleague in distress, and collect information in a trauma-informed way.
- **Ensure** that managers' training prepares them to check in regularly on distressed colleagues' well-being, as well as their digital security and physical safety needs.
- **Highlight** the importance of a trauma-informed approach to incident response, which may include, for example, training managers and editors to carefully collect information to minimize re-traumatization through retelling.
- **Outline** expectations and next steps for the targeted individuals so they are aware of what comes next, and what type of support they will be receiving.
- **Respect** the privacy of the targeted individual and ask for consent to share with other parties before doing so.
- **Emphasize** the need to manage one's own well-being and mental health while supporting others.

Cost & Organizational Size $$ - $$$

Costs for **staff time and/or consultancy fees**. Trauma-informed training and resources for managers and editors generally require a financial investment and is more practical **for mid-sized to larger organizations**; however, some free and low-cost resources are available that can be useful for newsrooms of all sizes.

Resources and Examples:

- Vita Activa's support and psychological first aid for journalists
- IPI's Online Course on Building an Effective Protocol for Newsrooms to Address Online Harassment
- Johns Hopkins University's Psychological First Aid training
- Shorenstein Center's article about how newsrooms' need to do more to protect journalists from online harassment
- Coalition Against Online Violence maintains a list of organizations that provide training, including PEN America, IWMF, IPI, CPJ, and ACOS Alliance

12. Educate Staff & Freelancers on Allyship

What:

Educate staff and freelancers about how to serve as allies to colleagues facing online abuse.

Why:

Online abuse is often intended to push journalists out of their profession, damage individual and organizational reputations, divide organizations internally, and undermine a free press. Providing staff and freelancers with guidance on effective and safe forms of allyship can bolster online abuse defense efforts and foster a culture of solidarity and peer support.

How:

- **Provide** guidance to staff and freelancers on practical ways to support colleagues by pointing them toward resources. (See "Document and Delegate.")
- **Highlight** the importance of checking in with the person facing abuse and centering their needs before taking any public-facing stance.
- **Inform** staff and freelancers on the various forms of public and private support the organization can provide—and the risks associated with each.
- **Offer** allyship training to leadership, management, staff, and freelancers.
- **Support** reporters who wish to investigate their colleague's attacker. This should be done in close consultation with the targeted individual to ensure their input and consent.

Cost & Organizational Size $ - $$

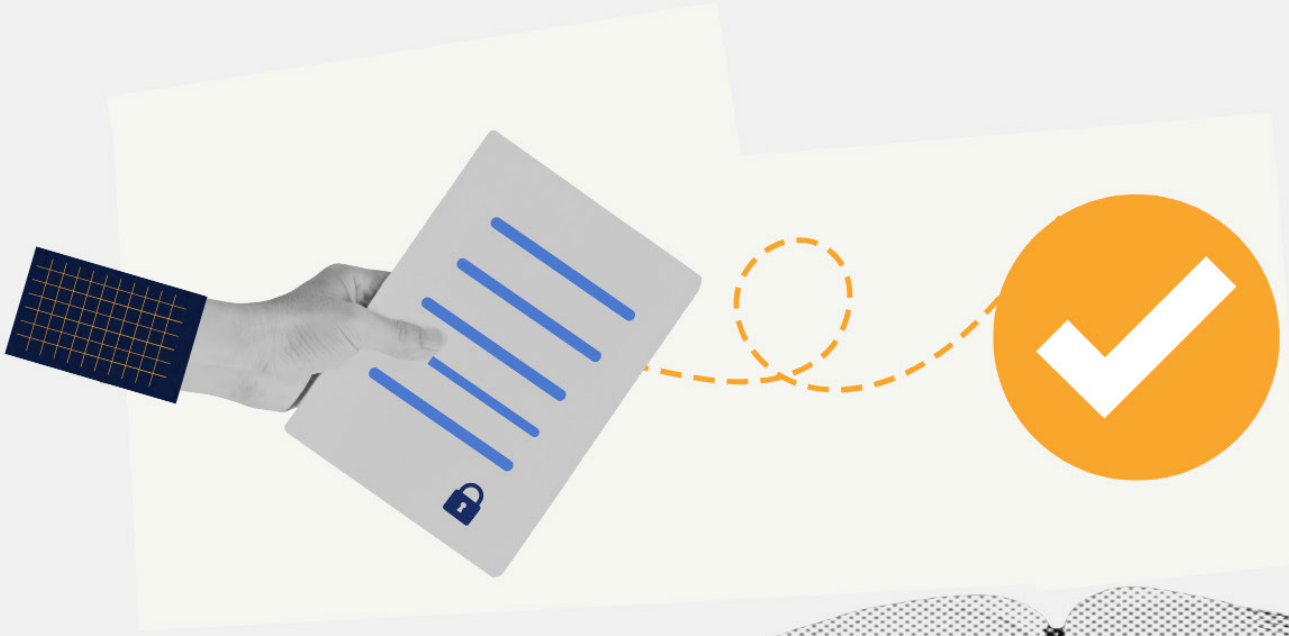
Costs for **staff time and/or consultancy fees. All news organizations** can benefit from providing allyship training and resources for staff and freelancers. While training may require financial investment, some useful resources are free.

Resources and Examples:

- Right to Be's allyship training program
- PEN America's Best Practices for Allies and Bystanders
- Johns Hopkins University's Psychological First Aid training
- OpenNews's Source project's How To Be an Ally in the Newsroom

Best Practices

For Managers and Editors



1. Reach Out and Listen

What:

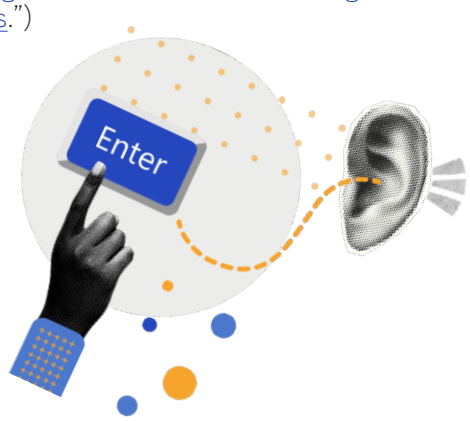
Proactively reach out to staff and freelancers to discuss online abuse, check in regularly, and understand their experiences and needs.

Why:

Online abuse can be profoundly isolating, disempowering, and traumatizing. Creating an environment of trust and safety ensures that staff and freelancers feel comfortable seeking support, and that people throughout the organization understand the issue.

How:

- **Build** trust over time by regularly creating space for staff and freelancers to voice concerns or recount experiences with online abuse. Check-ins could take place at cross-departmental, team, or weekly one-on-one meetings.
- **Schedule** regular safety check-ins for every relevant story or project. (For example, when a story is assigned, ask the journalist if they have safety questions or concerns, including about online abuse, and check in again once the story is published.)
- **Prioritize** the concerns of targeted individuals experiencing a specific incident by checking in privately and centering their needs. Remember that some individuals may feel uncomfortable disclosing or calling attention to their situation. In such cases, offer to include a trusted colleague or HR representative.
- **Engage** targeted staff and freelancers in every decision that could affect them, particularly regarding public disclosure and interactions with law enforcement.
- **Seek** training. If your organization offers training on how to provide trauma-informed support to your staff and freelancers, take advantage of it. If your organization does not offer such training, request it and/or seek out free online resources. (See "Provide Training and Resources for Managers and Editors.")



Cost & Organizational Size

Costs for **staff time and/or consultancy fees**. All news organizations can benefit from implementing regular check-ins and creating a culture of care, especially about safety and security.

Resources and Examples:

- Vita Activa's peer support and psychological first aid for journalists
- IPI's Newsrooms structures and support mechanisms / Communications
- OpenNews's Source project's How To Be an Ally in the Newsroom
- IWMF's Mental Health Guide for Journalists Facing Online Violence

2. Assess Risk and Response

What:

Work closely with staff and freelancers to assess the level of risk that they, their colleagues, and their families face. Risks may differ based on their identity, their beat, and the sensitivity of specific projects.

Why:

By proactively thinking through risks as a regular part of the reporting process, organizations can more effectively prevent, respond to, and mitigate those risks. Regular risk assessments can also build knowledge for long-term security planning and policy, normalize safety planning, and present an opportunity to remind staff and freelancers of available resources and appropriate communication channels.

How:

- **Think through** interrelated issues such as physical safety, digital security, legal risk, reputational damage, an organization's history and context, and even the safety and behavior of a reporter's sources and family members. Consider that both an individual target and the news organization might be subject to risk. It can be helpful to take into account developing trends and tactics, the stories that are most likely to generate abuse, and the reporters who have already been targeted online (and are therefore more likely to be targeted again).
- **Adapt** an established risk assessment template (see Resources and Examples, below) to your needs.
- **Consider** that the targeted individual may have their own resources that they prefer to consult, especially if they are more familiar with their community, subject area, and support system than their manager.
- **Consider** consulting in-house security, bringing on external security, engaging law enforcement, and/or providing temporary relocation as needed.
- **Consult** targeted individuals about every security decision that affects them. Debrief them once the story has been published.
- **Use** the information gleaned from risk assessments and debriefs to determine which abuse mitigation strategies are effective and which need improvement. Adjust organizational policies accordingly.

Cost & Organizational Size $ - $$$

Costs for **staff time and/or consultancy fees**. All news organizations should work with staff and freelancers to assess risk. Basic risk assessments require an investment of time, but free resources and templates are available. Higher-risk situations may require speaking with a safety expert, which may require more substantial financial investment.

Resources and Examples:

- IWMF's Online Violence Risk Assessment template
- Australian Broadcasting Corporation's guidelines on how to consider social media safety when commissioning content
- IWMF, IPI, and CPJ offer detailed guidance on risk assessment for newsrooms
- Columbia Journalism Review's Risk Assessments Can Make Journalism Safer
- CPJ's Editors' checklist: Protecting staff and freelancers against online abuse

3. Document and Delegate

What:

Offer staff and freelancers hands-on help with documenting and navigating online abuse, which may involve delegating support to the social media team, trusted colleagues, or external supporters.

Why:

Documenting online abuse is important for tracking patterns, including escalation, and for seeking support from law enforcement, security teams, and legal counsel. But it can be traumatizing and exhausting. Delegating some tasks can allow the targeted individuals to take a break for the benefit of their mental health and well-being.

How:

- **Provide** hands-on help for: documenting the abusive content; monitoring platforms for mentions (including by setting up Google Alerts); reporting, blocking, restricting, muting, and filtering abuse; and reviewing abusive content.
- **Spread** the burden of documentation among multiple allies if possible, to reduce exposure and potential secondary trauma.
- **Share** guidance on how to effectively document online abuse and make sure that all allies are familiar with the process.
- **Use** the delegated access feature, a secure way of sharing account access that's available on many platforms, including Gmail, Facebook (for pages but not profiles), Instagram (for business accounts only), and LinkedIn (for pages but not profiles).
- **Seek** support for targeted individuals from inside the news organization (colleagues, communications, etc.) or from external sources (NGOs, companies, etc.)

Cost & Organizational Size $ - $$

Costs for **staff time and/or consultancy fees**. Documentation often requires a relatively modest investment of staff time, but may occasionally require external support from nonprofits, external companies, or consultants.

Resources and Examples:

- PEN America's Guidelines for Talking to Friends and Allies and Best Practices for Allies and Bystanders

4. Communicate Policies, Protocols, and Resources

What:

Make sure staff and freelancers are aware of and can easily access the organizational policies, protocols, and resources for online abuse, digital safety, and social media (see "Develop Policies and Protocols").

Why:

In the midst of an attack, it can be difficult for impacted individuals to familiarize themselves with new policies, protocols, and resources. Requesting help is much easier if the process is clear, familiar, well-established, and regularly communicated.

How:

- **Remind** staff regularly of existing policies, protocols, and resources in meetings, at check-ins, during assignment risk assessments, and as PSA-style announcements at staff events.
- **Append** a note about these resources to different kinds of internal communications—from onboarding documents and email footers to the backs of press IDs and as notices hung in shared physical spaces, like coffee areas and restrooms.

Cost & Organizational Size

Costs for **staff time and/or consultancy fees**. All news organizations with established policies, protocols, and resources can regularly remind staff and freelancers of them at no cost.

Resources and Examples:

- BBC's Health and Safety Information Intranet for Staff

5. Seek Internal and External Support

What:

Seek support and consultation from internal or external experts, which may include communications, IT, HR, legal counsel, digital and physical security experts, and professional contacts at social media platforms.

Why:

Cases of online abuse sometimes involve physical safety, digital safety, legal considerations, psychological trauma, and reputational issues. Knowing what internal and external expertise is available and how to seek it enables more effective advocacy and support for those facing abuse.

How:

- **Consult** with your network about online abuse, asking what they have witnessed or experienced and how they handled it. Create a list of internal and external experts, which could encompass communications, PR, legal counsel, law enforcement, and physical security experts as well as professional contacts at social media platforms and technology companies.
- **Seek** the advice of civil society organizations (see "Resources and Examples" below), other media companies, professional associations, and commercial entities willing to provide discounted or pro bono support, especially if your organization lacks resources and in-house safety expertise.
- **Reach out** to professional contacts at social media platforms if you have them—*after* reporting the specific abusive incident through the platform's public reporting mechanisms.
- **Collect** relevant communications, documentation, and any information (such as links, account handles, and screenshots) that platforms might need to address individual incidents (see "Document and Delegate").

Cost & Organizational Size $ - $$$

Costs for **staff time and/or consultancy fees**. Smaller organizations can leverage in-house expertise, peer expertise, and low-cost or free external resources (see "Resources and Examples" below). Larger organizations can consult and outsource support to external partners. High-risk situations may require higher financial investment.

Resources and Examples:

- Coalition Against Online Violence's Resource Hub
- PEN America's Digital Safety program and Best Practices for Employers
- CPJ's Emergency Assistance team
- Freedom of the Press Foundation's Digital Security program
- IWMF's Newsroom Safety Training and Safety Consults
- IPI's Trainings for Journalists and Newsrooms on How to Combat Online Harassment and Investigate Disinformation
- Facebook's Trusted Partner program

Additional Resources

- PEN America's Best Practices for Employers and Online Harassment Field Manual
- Shorenstein Center's Tips for Newsrooms to Support Journalists Targeted by Online Harassment
- International Press Institute's Newsrooms OnTheLine
- International Women's Media Foundation's Guide to Protecting Newsrooms and Journalists Against Online Violence, Mental Health Guide for Journalists Facing Online Violence, and Better Protection for Freelancers Facing Online Violence
- Women's Media Center's Online Abuse 101 and What Online Harassment tells us about our newsrooms: From individuals to institutions
- Committee to Protect Journalist's Editors' checklist: Protecting staff and freelancers against online abuse
- #NotOk project's Newsroom Guide for Managing Online Harm, Tip Sheets for Individuals, and Identifying the Extent of Online Harm and Its Different Forms
- Coalition Against Online Violence's Resource Hub

Best Practices for News Organizations:
How to Protect and Support Journalists Harassed Online

PEN AMERICA

Coalition Against Online Violence

Acknowledgments
Design by Angie Caballero
Editing by Susan Chumsky