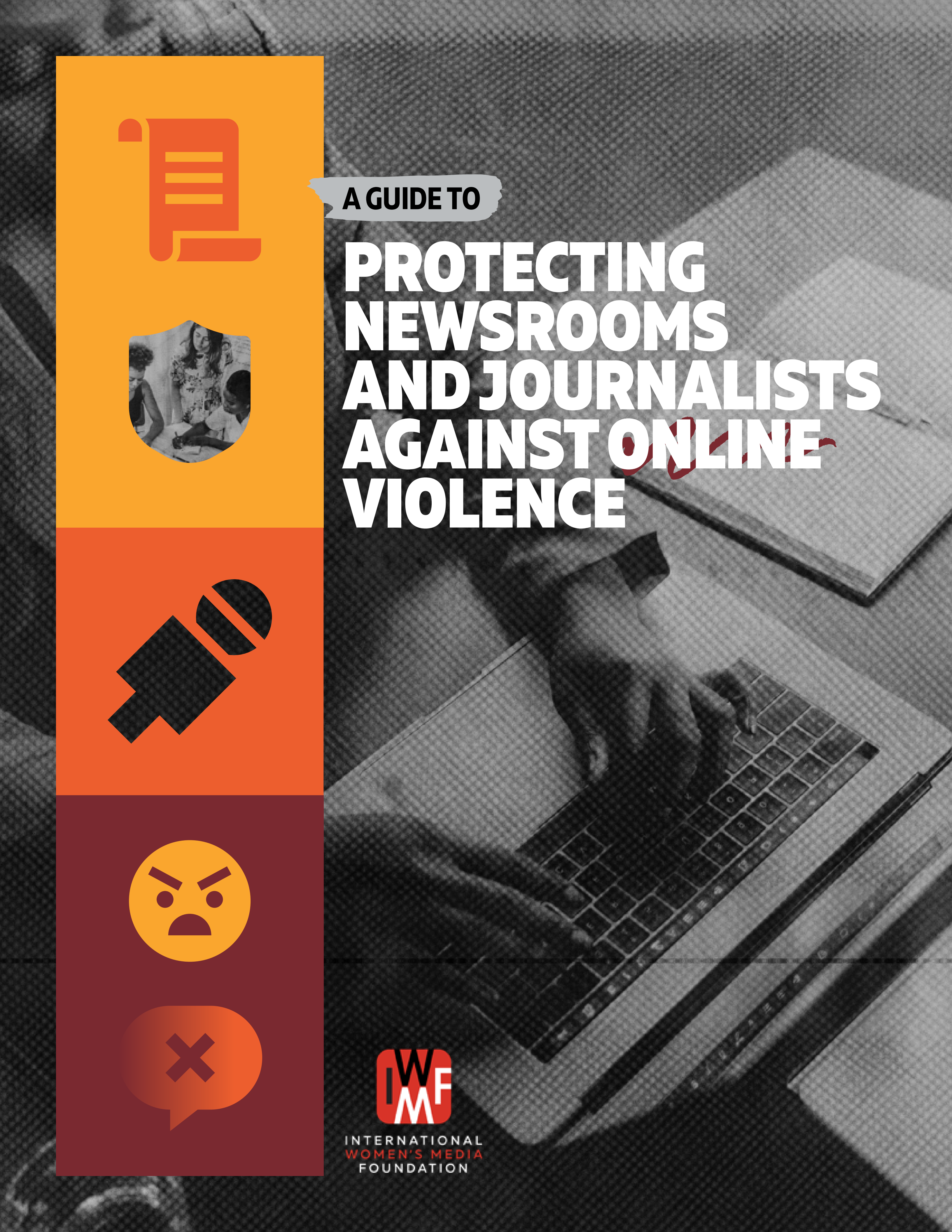


A GUIDE TO

# PROTECTING NEWSROOMS AND JOURNALISTS AGAINST ONLINE VIOLENCE

IWMF

INTERNATIONAL
WOMEN'S MEDIA
FOUNDATION

# ACKNOWLEDGEMENTS

This guide was created by Ela Stapley on behalf of the International Women's Media Foundation, September 2022.

**WITH THANKS TO:**

Anchorage Daily News
Bhekisisa
Clarín
Protocol Media
Radio Free Europe/Radio Liberty
The Seattle Times

**Design by:**
Estudio Salmon

The development of this guide was made possible with the support of Craig Newmark Philanthropies.

# TABLE OF CONTENTS

# FOREWORD

Online violence is the silent scourge of the newsroom. For too long journalists have endured constant harassment, resulting in serious implications for press freedom, including self-censorship. This abuse disproportionately affects women and diverse journalists who are often reluctant to speak out for fear of jeopardizing their careers. This culture of silence results in inadequate support from newsrooms for both staff and freelancers who are targeted simply for doing their jobs. Fortunately, as newsroom management becomes more aware of online abuse and its impact, policies and best practices are being implemented in an attempt to better protect employees.

The International Women's Media Foundation (IWMF) is dedicated to promoting a culture of change in newsrooms when it comes to tackling online violence. As part of our ongoing work with media outlets, we have supported newsrooms around the world with the development of guidelines to combat online abuse. In 2020, the IWMF created the Coalition Against Online Violence (CAOV), a growing body of more than 60 organizations working to find better solutions for women journalists facing online abuse; in 2021, the Coalition launched the Online Violence Response Hub, housing comprehensive resources and guidance for journalists facing online attacks.

## ABOUT OUR PILOT PROJECT

Over the past six months, we have worked with a wide range of newsrooms – from small specialized outlets covering health in South Africa to established independent newsrooms in the United States. All faced similar threats when it came to online harassment and all were looking for a better way to protect their staff.

No newsroom is the same, so before creating the online abuse policies, we spent time working with management to understand what the outlet needed, how they could implement change and how we could best support a shift in culture. Not all newsrooms needed the same level of support: for some outlets, our support was a light touch involving several meetings with management, help creating a resource or policy and a training session. For others, support was more in depth and involved round-table discussions with senior management, several training sessions for staff and guidance on creating an online abuse guide for staff with a number of different policies. Our work with these newsrooms is featured in case studies throughout this guide.

# ABOUT THIS GUIDE

There is no one policy that successfully tackles online violence; instead, a number of different guidelines are needed to protect staff. This guide includes some of the most commonly requested policies by newsrooms over a six-month period. It was created to meet the need of newsrooms for easy-to-implement templates that they could use within their own outlet.

## WHO IS THIS GUIDE FOR?

This guide is designed for newsroom management who want to create and implement online abuse policies to better protect their staff.

**The guide will:**

- Help you think through which policies are best suited to your newsroom
- Provide you with stand-alone policy templates you can adapt to the needs of your outlet
- Provide you with guidance and a template to create your own online abuse guide for the newsroom
- Suggest best practices and content to include when drafting your policies

## HOW TO USE THIS GUIDE

The layout of this guide is intended to be a roadmap for newsroom management looking to implement support for journalists experiencing online abuse. It starts with guidance on how to raise awareness and finishes with a template for creating your own online abuse manual.

**The guide contains:**

- Online templates for different policies that newsroom managers can adapt to the needs of their staff (newsrooms do not have to use each policy, instead they can pick and choose the ones best suited to the size and structure of their newsroom.)
- Guidance on what to include when writing your policies
- Case studies of the newsrooms we supported

## HOW TO USE THE ONLINE TEMPLATES

This guide has online templates that you can adapt to meet the needs of your newsroom. To use the online template follow the guide below.

Go to the template sections in this guide and follow the instructions to access the document online. You will need to make a copy of the file in order to be able to edit it later.

**To make a copy of a file:**

1. On your computer open the template you want to make a copy of.
2. In the menu, click **File** › scroll down to **Make a copy**.
3. Create a name for your document and choose where to save it.
   If you want to copy comments from a document, spreadsheet, or presentation, click **Copy comments and suggestions**. You can choose to include resolved comments and suggestions in your new copy.
4. Click **Ok** or **Make a copy**.

Now you will be able to edit/adjust the template.

**You can also download a copy of the templates, here is how:**

1. On your computer, open the template you want to download.
2. At the top, click **File** › **Download**.
3. Choose a file type. The file will download onto your computer.

## CONCLUDING WORDS

While this guide addresses a number of the policies that newsrooms need, it is not by any means complete. This guide does not include policy and best practices for documenting abuse or guidance for media outlets working with freelancers, nor does it address the wellbeing and mental health of journalists targeted by online harassment. These issues are covered in excellent resources by other CAOV members and are featured at the end of this **guide**.

This guide could not have been created without the insight and learnings from the newsrooms featured as case studies. The IWMF would like to thank these outlets for their participation in our pilot project and congratulate them on being among the first newsrooms worldwide to step up and tackle online violence.

# WHAT WE LEARNED FROM WORKING WITH NEWSROOMS

Our preliminary work with different newsrooms gave us a good understanding of what works and what doesn't work when it comes to successfully implementing change around online abuse. We have included these learnings below as an aid for other newsroom managers who are thinking about how to implement best practices for protecting against online abuse.

## FIND YOUR NEWSROOM CHAMPION

All of the newsrooms we worked with had one or two people in management who were extremely dedicated to pushing for change when it came to finding solutions to online violence. They were not only passionate about change but were flexible about finding solutions to ensure a culture shift, including working with other departments in the newsroom.

## GETTING BUY-IN FROM UPPER MANAGEMENT

Change is difficult to implement if upper management does not understand the scope of the problem. To ensure long-term change, it is important that upper management is engaged in the process of supporting staff who are targeted by online abusers. Raising awareness of the issue can be done in a number of ways, which we have outlined in the next chapter.

## SIZE OF THE NEWSROOM

The size of the newsroom matters when it comes to implementing change. Bigger, more established newsrooms need to include more stakeholders when it comes to drafting and implementing policies, which can take time. Smaller newsrooms are more nimble, but may be lacking important areas of support, such as an Information Technology (IT) department.

## WORK WITH MIDDLE MANAGEMENT

A number of the policies require the support of middle management. These are normally editors who will be the first point of contact for staff looking to raise concerns around online abuse. Ideally, they should be included in the policy-making process from the outset.

## WORKING WITH OTHER DEPARTMENTS

Similarly, a number of policies rely on the participation of different departments in the newsroom, including Human Resources (HR) and IT. Establishing a contact who will work with you to implement change is key to rolling out successful best practices.

## UNDERSTAND THAT YOUR STAFF USE THEIR PERSONAL ACCOUNTS FOR WORK CONTENT

Journalists use their personal social media accounts for work, yet receive little guidance on how to protect those accounts or their own personal data. All the newsrooms we worked with saw the importance of providing this support to staff.

## TRAINING

Building skills through regular training is an important part of ensuring long-term success in protecting staff against online harassment.

CHAPTER 1

# RAISING AWARENESS OF ONLINE VIOLENCE IN THE NEWSROOM

# WHY IT'S IMPORTANT TO RAISE AWARENESS

**Online abuse disproportionately affects women and diverse journalists, who often do not hold upper management positions and are often reluctant to report harassment. As a result, management may be unaware of the damage online attacks are doing both to staff and to the media outlet. By raising awareness of what online violence is and how it impacts staff and press freedom, the newsroom will be in a better place to protect against it.**

# HOW TO RAISE AWARENESS

## FRAME IT AS A GLOBAL PROBLEM AND A PRESS FREEDOM ISSUE

Our work with newsrooms found that holding round-table discussions with management, in which we looked at the global picture of online abuse and its impact on press freedom, was the most effective way of raising awareness. Online abuse has serious consequences for freedom of expression and the journalists' ability to do their job. Putting this issue in perspective allowed newsrooms to think more openly about how to support staff.

## WAYS OF RAISING AWARENESS

There are a number of ways to both raise and maintain awareness of online abuse in the newsroom, including:

- Working with an external organization to facilitate discussions with management
- Training for staff and management
- Raising the issue of online abuse in staff meetings and one-on-one editorial meetings
- Creating a guide to combat online abuse and being proactive about sharing it with the newsroom
- Visualizing online abuse by using real-life case studies from staff in the newsroom. (Please ensure you have their permission before sharing their stories.)
- Creating a Slack channel, WhatsApp group or other messaging group where users can share best practices and tips as well as flag any possible upcoming abuse as a result of a story

# WHAT TO CONSIDER WHEN RAISING AWARENESS

- Raising awareness should ideally be the first of many steps the newsroom takes to address online violence. Change in the newsroom works best when it is accompanied by practical support for staff.

- It's important to set clear goals for what you want to achieve when it comes to raising awareness. Be realistic about what your media outlet will be able to do in the short, medium and long term.

- Be clear with staff about what support your newsroom will offer and when.

- Identify key allies in the newsroom who will work with you to raise awareness as well as create and integrate policies and best practices. Working with other departments, such as HR and IT, will ensure a much more integrated approach to supporting staff.

- Often the burden of raising awareness falls to those who are being targeted by online attackers. It is important that this hardship is recognized, that these staff are supported and that other members of the newsroom are involved in tackling the issue.

- Consider bringing in outside help from organizations specializing in dealing with issues around online abuse.

- Think about how you will raise awareness in both the physical space of the newsroom (ex: printing out and distributing information), as well as the digital space (ex: letting people know where they can find online abuse policies and guides).

CASE STUDY

# RAISING AWARENESS OF ONLINE VIOLENCE USING A ROUND-TABLE DISCUSSION

We supported Radio Free Europe/Radio Liberty with the development of online violence guidelines and training over a period of six months. This case study focuses on one area of our support: facilitating a round-table discussion with management as a way to raise awareness.

## RADIO FREE EUROPE/RADIO LIBERTY (RFE/RL)

### ABOUT THE NEWSROOM

Number of journalists in the newsroom:

**600 full-time journalists and around 1,300 freelancers**

Location:

**Prague, Czech Republic. Twenty local bureaus including Ukraine, Georgia and Kyrgyzstan.**

Type of newsroom:

**Multiplatform media company, engaging audiences on digital platforms, TV and radio. News provided in 27 languages and in 23 countries in Europe and Asia.**

## HISTORY OF ONLINE ATTACKS

Journalists in RFE/RL newsrooms face a wide range of different online attacks from well-organized adversaries. The vast geographical distribution of their bureaus means that the media outlet needs to support staff who are targeted by governments, extremist groups, political zealots and everyday harassers; this assistance is no easy feat. Journalists are also targeted by misogynistic hate campaigns, hate speech and defamation campaigns. In some regions, bureaus are unable to publish content on social media platforms because governments exploit loopholes in social media community guidelines to undermine their ability to publish.

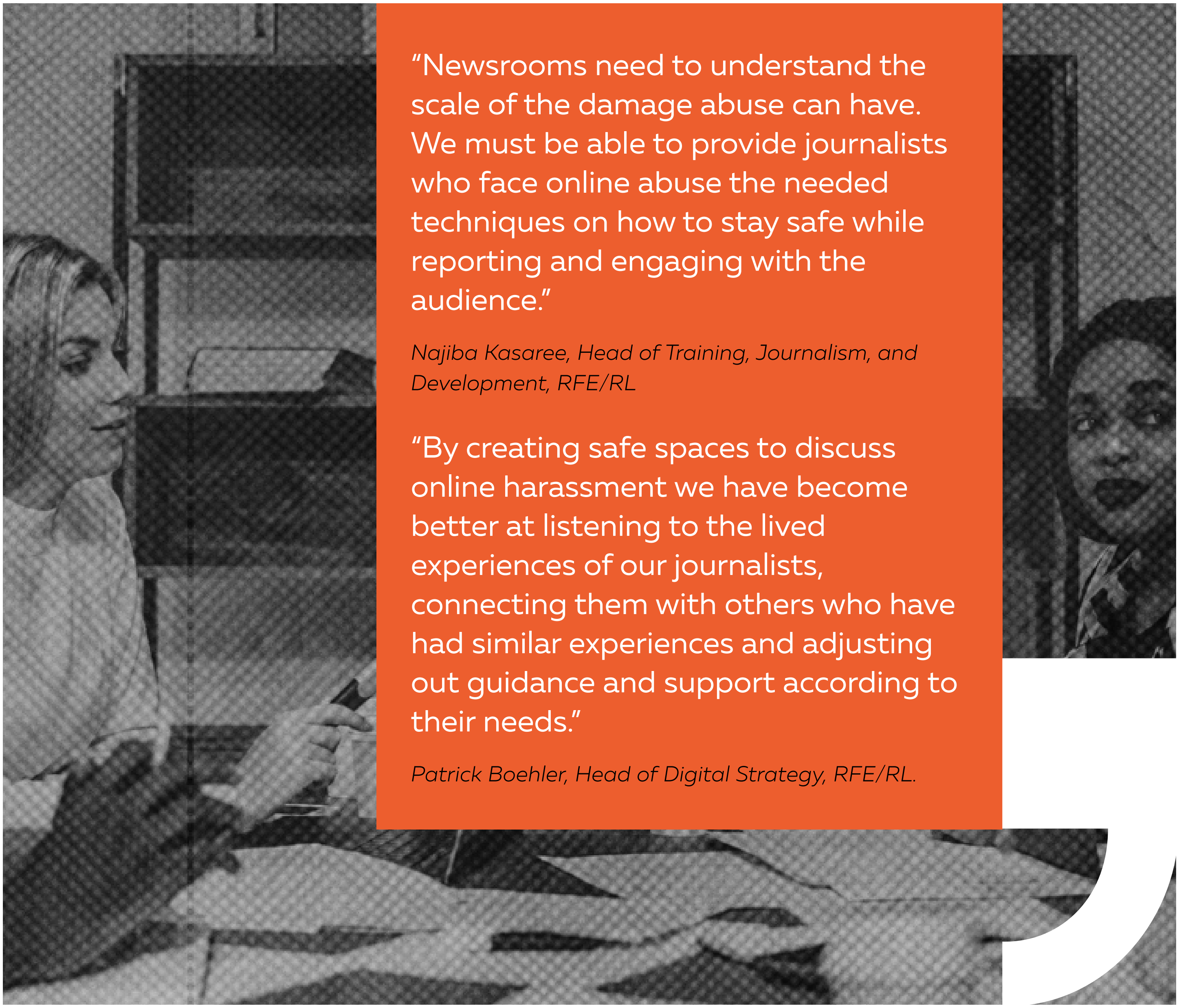
## OUR SUPPORT

RFE/RL's priority was to raise awareness about the seriousness of online abuse and its impact both on the newsroom and the ability of its journalists to do their jobs. Their need was complicated due the dispersed nature of their teams. Working with the Head of Digital Strategy, we designed and ran a round-table discussion for senior management and editors where we spoke about online violence in a global context and its threat to press freedom. This was helpful for conveying that online abuse is a systemic problem without a one-size-fits-all solution. By opening up the discussion, we were then able to provide training to two editorial teams working in regions where online abuse was being used as a censorship tool.

We also worked closely with the Head of Journalism, Training, and Development to facilitate a session for women journalists in the organization and their allies. This discussion was a safe space for them to share their stories and for us to provide guidance on how best to protect themselves online. We also created a checklist for protecting staff data, which RFE/RL will incorporate into its onboarding manual.

## WHAT HAPPENED NEXT

The outlet implemented a number of changes to the way it supports staff, including the creation of digital security guidelines, training, creating a channel on hate speech where staff can go to share experiences and expert guidance and community guidelines for their own commenting platform. It is currently working on an onboarding document for new hires and leadership has also created a new position, digital security evangelist – a role that will help journalists be safer in their day-to-day work.



"Newsrooms need to understand the scale of the damage abuse can have. We must be able to provide journalists who face online abuse the needed techniques on how to stay safe while reporting and engaging with the audience."

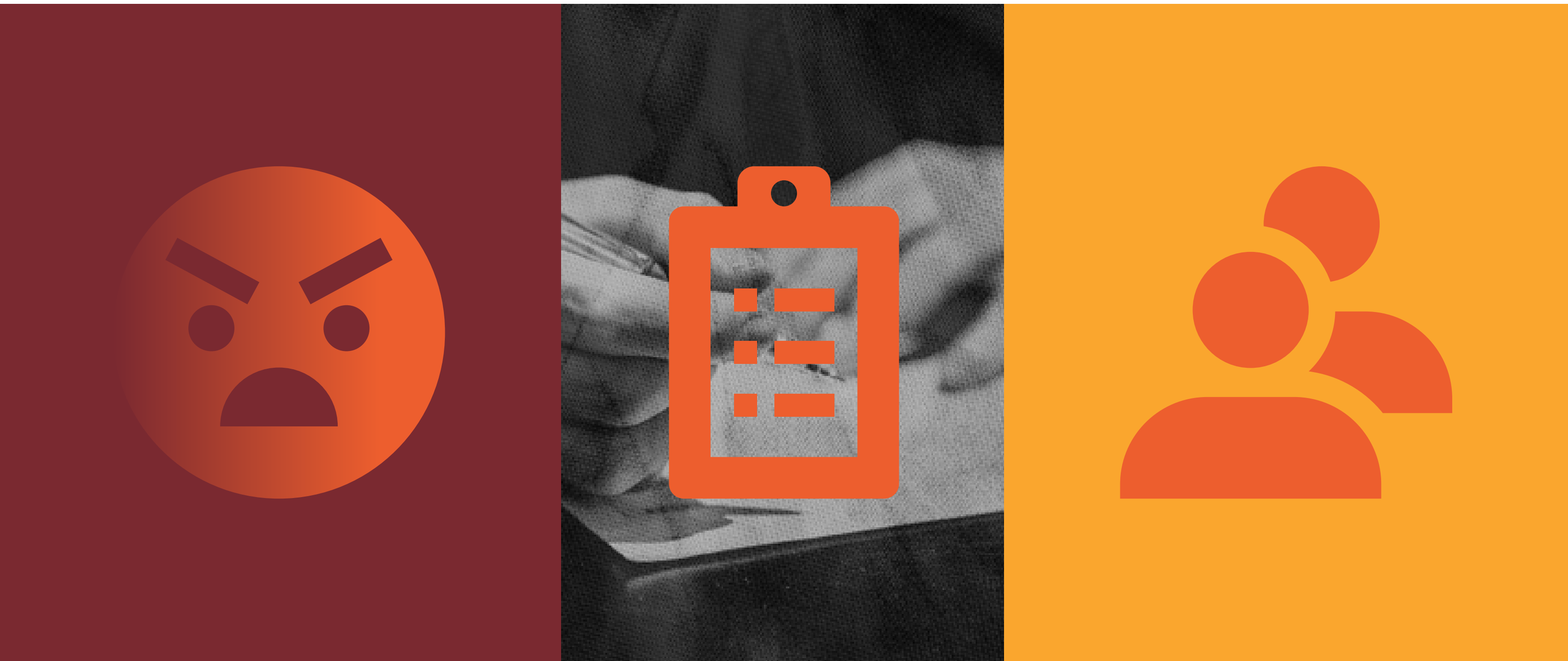
*Najiba Kasaree, Head of Training, Journalism, and Development, RFE/RL*

"By creating safe spaces to discuss online harassment we have become better at listening to the lived experiences of our journalists, connecting them with others who have had similar experiences and adjusting out guidance and support according to their needs."

*Patrick Boehler, Head of Digital Strategy, RFE/RL.*

CHAPTER 2

# STAFF SURVEY OF ONLINE VIOLENCE



# WHY CREATE A SURVEY?

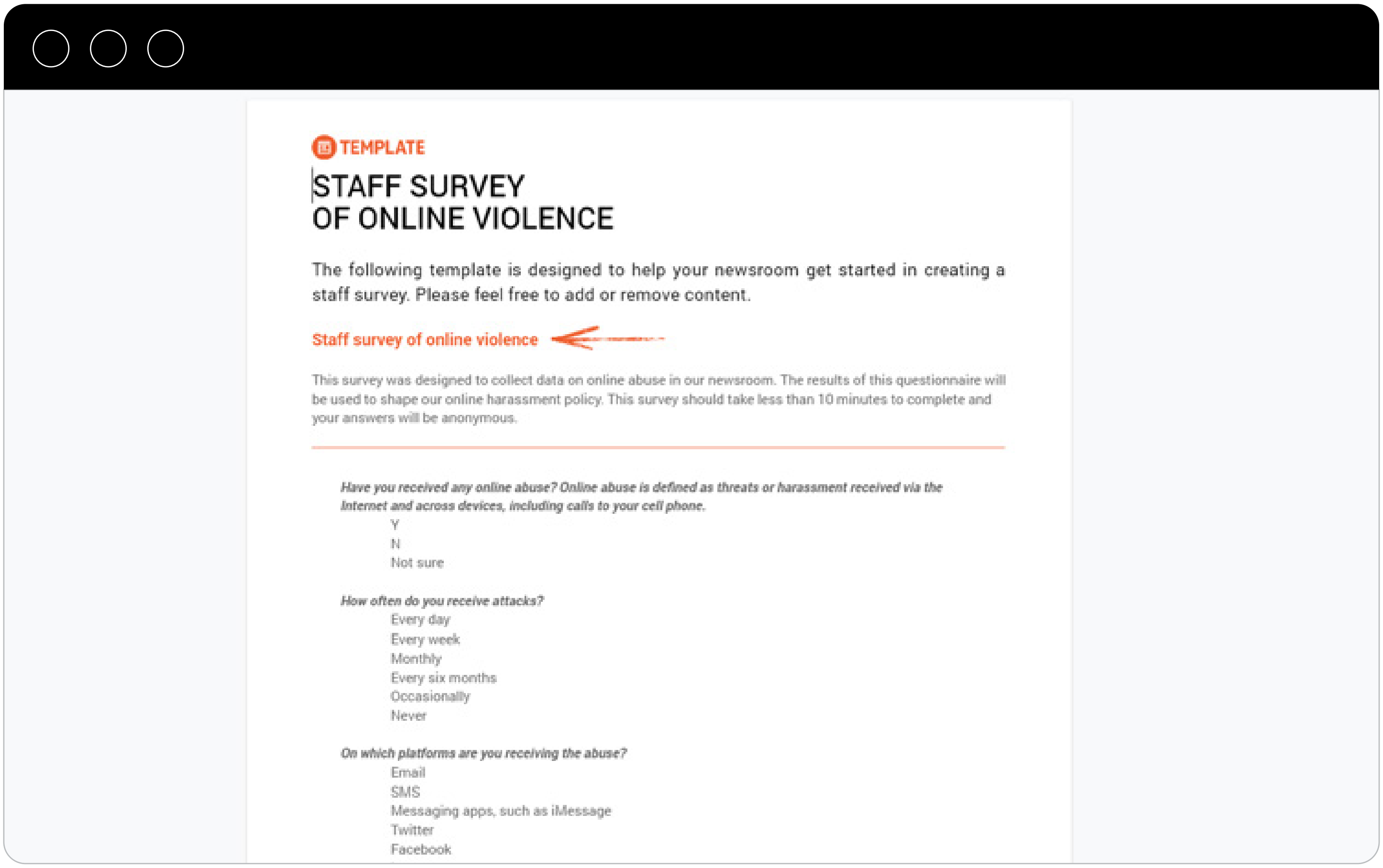
Those targeted by online abuse may not feel comfortable approaching management about the harassment they have received. Online violence disproportionately targets women and diverse journalists who often do not hold management positions within the newsroom and therefore may be reluctant to come forward. An anonymous survey can help management to understand the scale of the problem, which allows the newsroom to create the policies needed to address the issue and barriers to supporting staff.

# WHAT TO CONSIDER WHEN CREATING AND DISTRIBUTING A STAFF SURVEY

- Having an anonymous survey will encourage honest answers.
- Before creating the survey, think about the type of data you want to collect and why you want to collect it.
- Be mindful that collecting data, such as job title or beat, can reveal the identity of a person. If you want to find out if online abuse is affecting some departments more than others, it can be helpful to organize individual sessions with journalists once the general survey is complete.
- Use an online form, such as Google Forms, to create your survey.
- Keep the survey as short as possible to encourage people to respond.
- The survey should have an introductory paragraph clearly stating the aims of the survey, the time needed to complete it and what will happen once the results are collected.
- Be transparent with staff about why you are creating the survey.
- Send the survey to everyone in the newsroom, not just women or diverse groups.
- Set a realistic time frame for completing the survey and send a follow up reminder to staff kindly asking them to complete the survey and specifying why.
- Consider making the results of the survey available to staff.
- Use the results of the survey to help inform next steps when it comes to supporting staff and creating policies.
- Consider carrying out an anonymous survey on a yearly basis to ensure that management is well-informed around online abuse issues in the newsroom.

# STAFF SURVEY OF ONLINE VIOLENCE

The following template was designed to help newsrooms get started with their own survey. You can access and edit an online version of this form **here**



TEMPLATE

## STAFF SURVEY OF ONLINE VIOLENCE

The following template is designed to help your newsroom get started in creating a staff survey. Please feel free to add or remove content.

### Staff survey of online violence

This survey was designed to collect data on online abuse in our newsroom. The results of this questionnaire will be used to shape our online harassment policy. This survey should take less than 10 minutes to complete and your answers will be anonymous.

***Have you received any online abuse? Online abuse is defined as threats or harassment received via the Internet and across devices, including calls to your cell phone.***

Y
N
Not sure

***How often do you receive attacks?***

Every day
Every week
Monthly
Every six months
Occasionally
Never

***On which platforms are you receiving the abuse?***

Email
SMS
Messaging apps, such as iMessage
Twitter
Facebook

CASE STUDY

# CREATING A STAFF SURVEY

Concerns about online abuse and its impact on staff led the Anchorage Daily News to request assistance drafting online abuse policies. Initial conversations indicated that creating a staff survey would be the most effective way of understanding the scope of the situation in the newsroom.

## ANCHORAGE DAILY NEWS

### ABOUT THE NEWSROOM

Number of journalists in the newsroom:
**30**

Location:
**Anchorage, Alaska, U.S.**

Type of newsroom:
**Local/Regional news organization, online with a print edition six days a week**

## HISTORY OF ONLINE ATTACKS

Hostility directed toward newsrooms and journalists has increased within the past several years, and Alaska, U.S., is no exception. The newsroom has increasingly received attacks on its credibility, including coordinated campaigns by public officials or by their political supporters. These attacks happen via social media as well as through phone calls and messages. The ongoing harassment has had an impact on journalists' well-being, leading newsroom managers to create policies to better protect their staff.

## OUR SUPPORT

Anchorage Daily News reached out for guidance on how best to support staff with issues around online violence. It was important for them to understand the scope of the problem, which is why designing a staff survey was the best first step. The IWMF created a first draft with questions designed to obtain information on how often abuse was happening and through what medium. The managing editor then added questions tailored to the newsroom, including asking how the newsroom could better support staff.

## WHAT HAPPENED NEXT

The outlet plans to distribute the survey in the coming months and the answers will be used to shape future policies and identify barriers to providing support to staff. The newsroom will also be sharing a digital hygiene checklist developed with support from the IWMF and will also launch a dedicated Slack channel where staff can share resources for managing digital security and online abuse.

> "More of our journalists have spoken up about the attacks they have experienced, and our concerns extend to not only security issues, but the physical, mental and emotional well-being of our team."
>
> *Vicky Ho, Managing Editor, Anchorage Daily News*

> "The IWMF's support on this work has opened up the dialogue within our news organization with regards to digital abuse and harassment."
>
> *Vicky Ho, Managing Editor, Anchorage Daily News*

CHAPTER 3

# DIGITAL SAFETY AND ONLINE VIOLENCE

# DIGITAL SAFETY IN THE NEWSROOM

Different sized newsrooms have varying levels of support when it comes to digital security. While bigger newsrooms may have the support of an IT team responsible for securing the media's online infrastructure, smaller outlets may have outsourced their IT or have a member of staff designated to set up staff email and oversee the website. In both cases, there is generally little guidance on how to support staff targeted by online abuse. When it comes to online abuse, newsrooms – especially those with limited staff or IT knowledge – can focus on two areas of digital safety:

## 1. HELPING STAFF SECURE THEIR ONLINE DATA

With the growth of social media, journalists are encouraged to share information about themselves as a way of building their brand and connecting with an audience. This data is now being used by online abusers to harass and threaten media workers and their families.

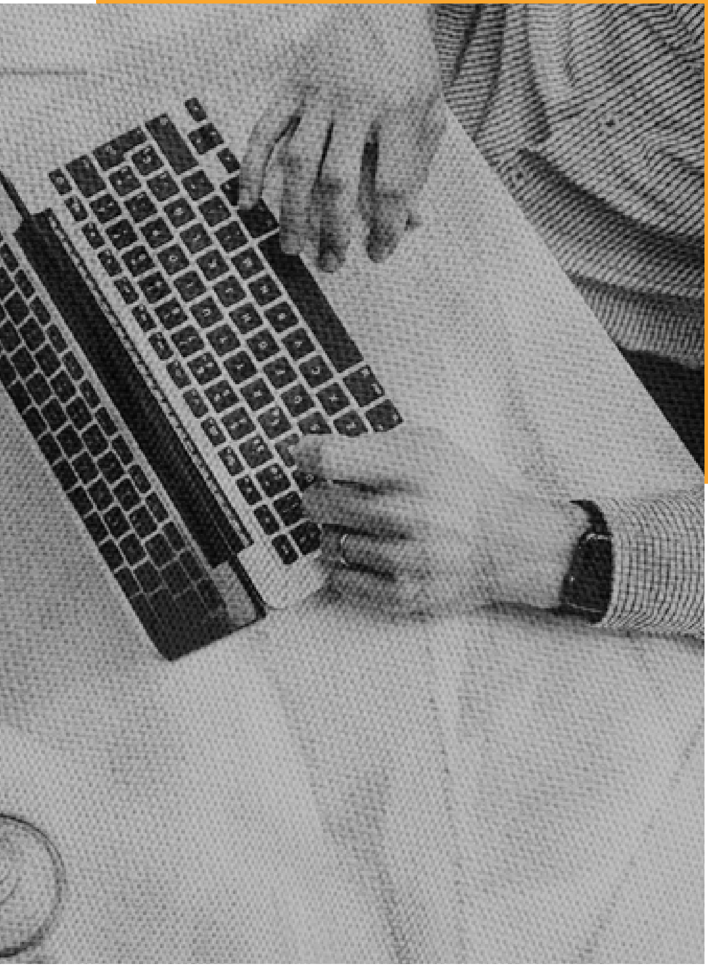
**Newsrooms can better protect journalists by:**

- Making journalists aware that certain forms of data are best kept private, including data used to locate them, contact them or data used to commit identity theft, such as a date of birth
- Letting journalists know that their online data can be used to harass them
- Using risk assessments and checklists to help journalists protect their data
- Having a designated person in the newsroom who can work with journalists to manage their online footprint
- Holding training for staff on how to better protect their online data
- Having clear policies that lay out what the media outlet will do in the event of a targeted online attack, doxxing or smear campaign

## REMOVING PERSONAL INFORMATION FROM DATABROKER SITES

Databroker sites hold a lot of personal data on people, including home address, cell phone numbers, and details on who lives in the same household. This data can be used to harass and threaten journalists.

A databroker removal service will delete that content. Signing journalists up for a repeated yearly subscription is the best way to protect their online information. Services, such as **Abine DeleteMe** is available in the U.S as well as a select number of other countries.



## 2. HELPING STAFF SECURE ONLINE ACCOUNTS

Journalists often use their personal social media accounts to publish their work and to engage with their audience. Traditionally, newsrooms have not taken the lead on helping journalists secure their personal social media accounts, which means that while their staff email may be secure, their Twitter accounts are not.

**Newsrooms can support staff by:**

- Understanding that a journalist's personal social media accounts are being used for work-related content and therefore need protecting
- Training them on the best ways to secure their personal accounts
- Providing them with in-house IT support to walk them through setting up two-factor authentication and printing out backup codes
- Providing them with support in setting up and using password managers

CASE STUDY

# DIGITAL SAFETY TO PROTECT AGAINST ONLINE VIOLENCE

As a newsroom focused on health and social justice, Bhekisisa started to receive significant online abuse while covering the COVID-19 pandemic, especially when public health measures such as wearing masks and vaccinations were implemented. Bhekisisa got in touch with the IWMF so we could help bolster its digital safety and create online abuse policies.

## BHEKISISA

### ABOUT THE NEWSROOM

Number of journalists in the newsroom:

**7**

Location:

**Johannesburg, South Africa**

Type of newsroom:

**An independent digital media organization focusing on health and social justice issues across Africa. Collaboration with partners who publish stories both online and in print.**

## HISTORY OF ONLINE ATTACKS

Staff at the newsroom, especially the Editor in Chief, were subjected to increased levels of online abuse as a result of their coverage of the Covid-19 pandemic. This includes the hacking of the Editor in Chief's Twitter account. These attacks appeared to be coming from global conspiracy theorists as well as anti-maskers and anti-vaxxers. The media outlet itself was also subjected to coordinated smear campaigns attempting to undermine the credibility of the organization. Those targeting the outlet focused on Bhekisisa's source of international funding as an attempt to undermine their work.

## OUR SUPPORT

We worked with the outlet over a six-month period to help fortify their digital safety with a focus on protecting staff data and securing their accounts, including their personal accounts. Bhekisisa does not have an IT department, so we created a policy for account security, including setting up and using two-factor authentication and printing out backup codes. We also guided them through the creation of a checklist for protecting staff data. This exercise was followed by a training session for staff on how to protect their data online. We also provided tailored digital security support for the Editor in Chief, which included a detailed guide on how best to protect her Twitter account.

## WHAT HAPPENED NEXT

Bhekisisa is now planning to share its online abuse policy with staff and will focus on building out mental health and well-being support using materials from the Online Violence Response Hub. We are pleased to continue working with the newsroom on a second phase focused on increasing the digital safety of its newsroom.

> “The IWMF training session was a great way to pinpoint all the ways we put ourselves at risk online. A social media presence has become a given in journalism but the risks are rarely discussed. I found the session very useful with lots of concrete, actionable ideas that are easy to put into practice. It’s definitely changed the way I think about the ‘occupational hazards’ of working in the news, which now include online attacks in my mind.”
>
> *Joan van Dyk, News Editor, Bhekisisa*

CHAPTER 4

# CHECKLIST FOR PROTECTING STAFF DATA

# WHY USE A CHECKLIST?

Checklists can be a useful way to help staff better protect their online data. Not only do they provide employees with clear steps on what to do, but they also show how staff can start to protect personal information. The IWMF put together a template checklist for reviewing, managing and securing data. This checklist can be used as a standalone document or in conjunction with the online violence risk assessment template in the next chapter.

# WHAT TO CONSIDER WHEN CREATING AND IMPLEMENTING A CHECKLIST

- Different countries have different data privacy laws and different rules around what data can be public facing. Media outlets should ensure these regulations are reflected in the checklist and that journalists are aware of what data can and cannot be removed legally.

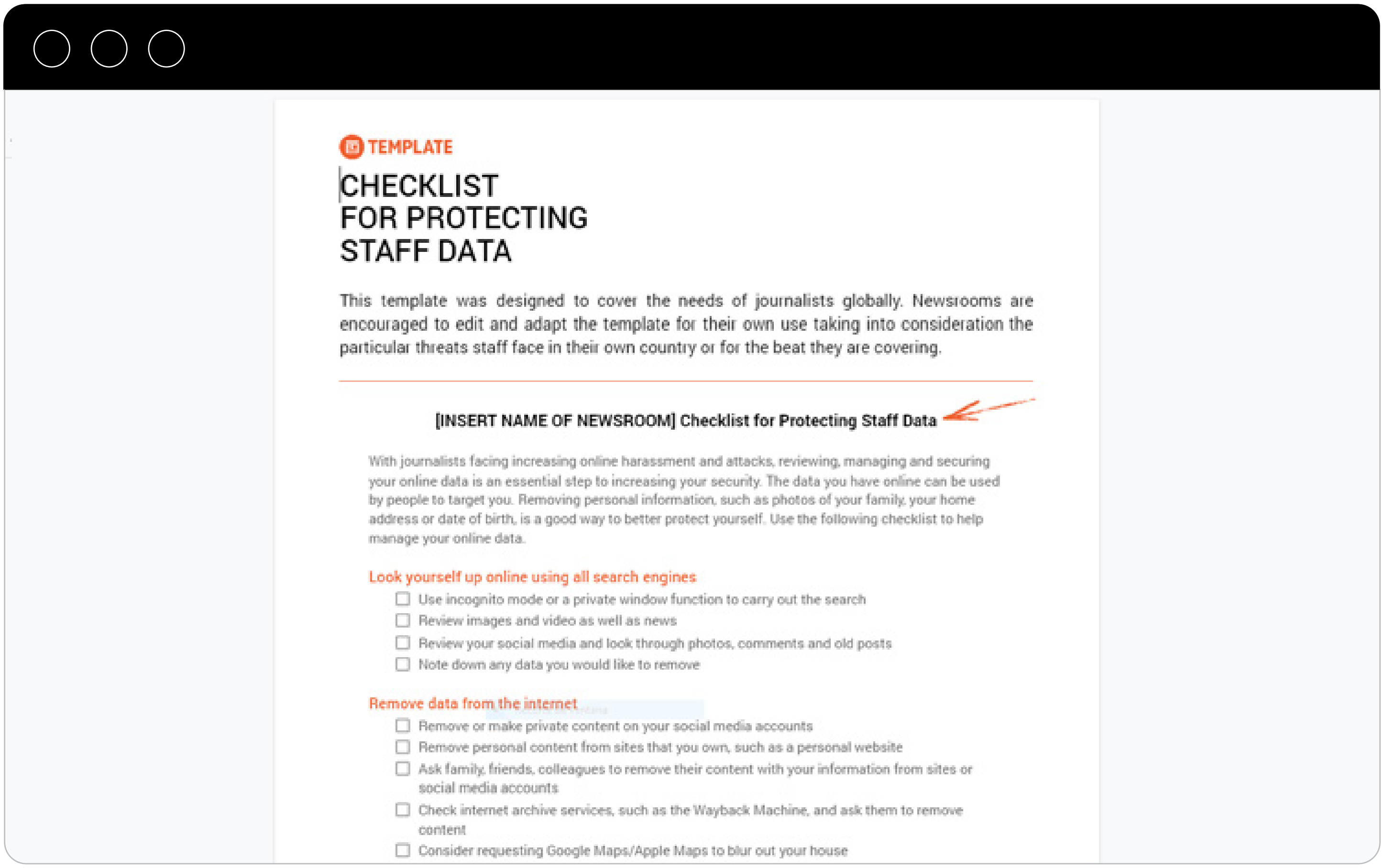
- The checklist includes advice on securing accounts. Newsroom management should ensure staff have been provided with guidance on how to secure their accounts. Please refer to the chapter on digital safety and online violence for more details.

- The checklist should be shared regularly with staff and should be located in a place that is easy for employees to access; for example, included in an onboarding manual, pinned to the top of Slack channel and/or stored on an internal server or in the Cloud.

- Newsroom managers should know when, and when not, to use the checklist. For example, it can be used when a journalist is covering a story with a high risk of online abuse.

# CHECKLIST FOR PROTECTING STAFF DATA

This template was designed to cover the needs of journalists globally. Newsrooms are encouraged to edit and adapt the template for their own use taking into consideration the particular threats staff face in their own country or for the beat they are covering. You can access an online version of this form here



TEMPLATE

CHECKLIST
FOR PROTECTING
STAFF DATA

This template was designed to cover the needs of journalists globally. Newsrooms are encouraged to edit and adapt the template for their own use taking into consideration the particular threats staff face in their own country or for the beat they are covering.

**[INSERT NAME OF NEWSROOM] Checklist for Protecting Staff 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.

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 private content on your social media accounts
- □ Remove personal content from sites that you own, such as a personal website
- □ Ask family, friends, colleagues to remove their content with your information from 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

CASE STUDY

# CHECKLIST FOR PROTECTING STAFF DATA

We were connected with Clarín through the Women in the News Network, a network promoting equal opportunities for women journalists through digital training and collaboration. We worked with the newsroom to provide them with basic online abuse training for staff as well as an easy-to-implement solution for protecting staff data. We also worked with them to create a checklist to protect staff data.

## CLARÍN

### ABOUT THE NEWSROOM

Number of journalists in the newsroom:
**350**

Location:
**Buenos Aires, Argentina**

Type of newsroom:
**The most widely read newspaper in Argentina and in the Spanish-speaking world**

## HISTORY OF ONLINE ATTACKS

Journalists working at Clarín are subjected to regular online harassment, especially those who are covering politics or gender issues. They receive harassment to their staff email as well as to their personal social media feeds. This includes acts of doxxing and the publishing of their personal data, such as an address, in an attempt to intimidate and threaten.

## OUR SUPPORT

This was a light-touch support partner that we worked with for one month to provide practical and simple guidance. We coordinated with the head of the Sustainability and Diversity Program to design a remote training session for journalists in the newsroom most affected by online abuse. This group included women journalists covering gender issues in Argentina and who are subjected to abuse on a daily basis. We also created a short checklist that the media outlet could integrate into onboarding documents.

> “It’s important for us to support our journalists with the tools they need in order to do their work safely. This checklist is a simple and practical solution for our busy newsroom.”
>
> *Nicole Insignares Nazzaro, CSR and Sustainability Manager, Clarín*

CHAPTER 5

# ONLINE VIOLENCE RISK ASSESSMENT

# WHY CARRY OUT A RISK ASSESSMENT?

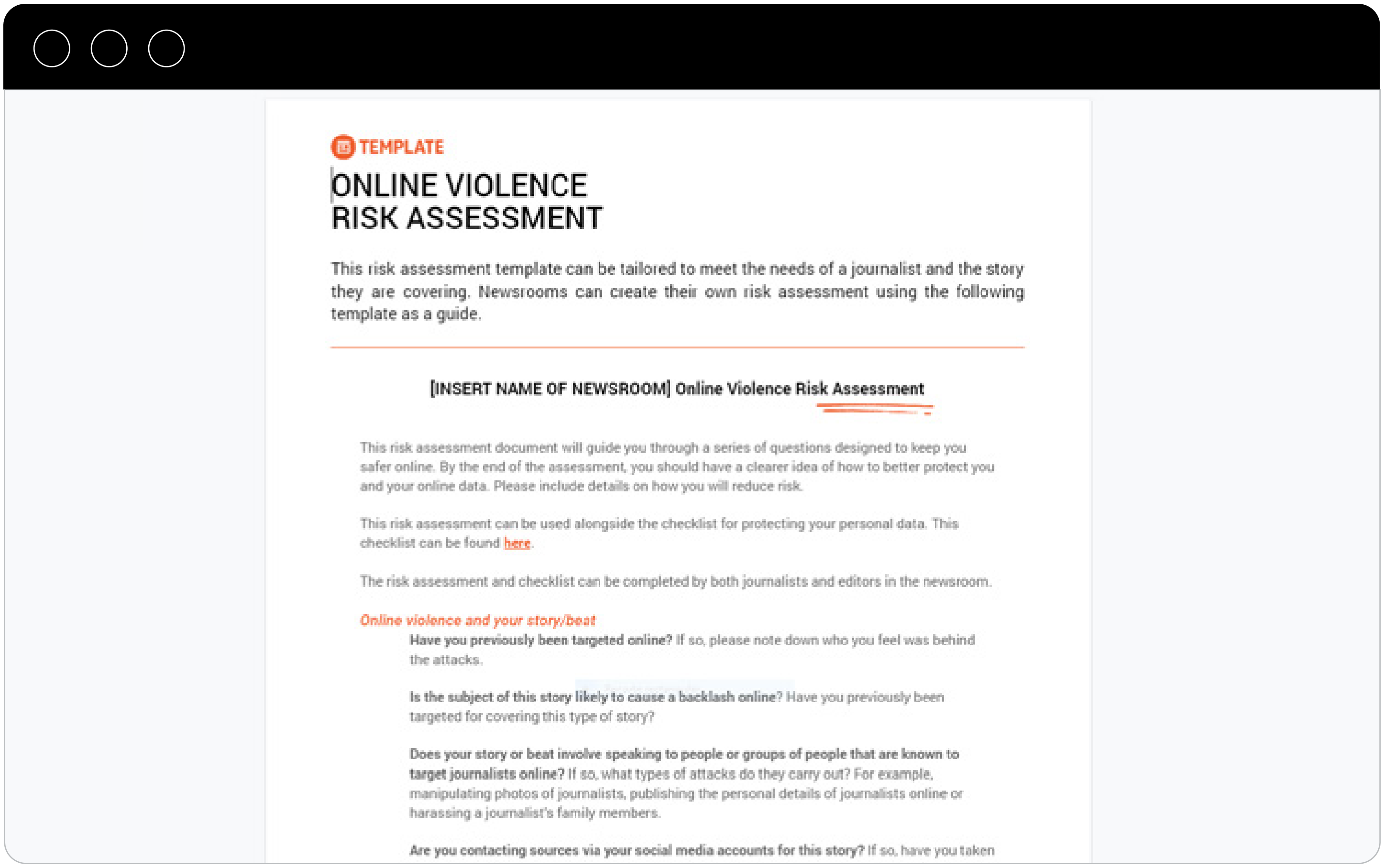
An assessment document can help mitigate risk when it comes to better protecting staff against online abuse. Upon completion of the risk assessment, journalists will know what steps they need to take to secure their online data and protect their accounts, as well as who in the newsrooms should be notified after abuse. The risk assessment document can be used with the **checklist for protecting staff data** found in the previous chapter.

# WHAT TO CONSIDER WHEN REVIEWING A RISK ASSESSMENT

- Work with the journalist to mitigate the risks rather than just identify them.
- Let them know what support is available in the newsroom and ensure they know who to go to if they need help managing issues around online abuse.
- Speak with the journalists about any online abuse they experienced from working on previous stories. Try to identify who may be behind the attacks and whether they are likely to attack again.
- Know that journalists who have previously been targeted online are likely to be targeted again, regardless of what stories they cover.
- Know that online abuse tends to increase during times of unrest, including during election campaigns.
- Knowing what type of stories result in online abuse will help you better protect journalists covering particular beats.
- Normalize speaking about online abuse so that journalists feel comfortable raising the issue.

# ONLINE VIOLENCE RISK ASSESSMENT

This risk assessment template can be tailored to meet the needs of a journalist and the story they are covering. Newsrooms can create their own risk assessment using the following template as a guide. You can access an online version of this form here



TEMPLATE

ONLINE VIOLENCE RISK ASSESSMENT

This risk assessment template can be tailored to meet the needs of a journalist and the story they are covering. Newsrooms can create their own risk assessment using the following template as a guide.

**[INSERT NAME OF NEWSROOM] 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 can be used alongside the checklist for protecting your personal data. This checklist can be found here.

The risk assessment and checklist can be completed by both journalists and editors in the newsroom.

*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?

**Does your story or beat involve speaking to people or groups of people that are 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

CHAPTER 6

# REPORTING AND ESCALATION POLICY

# WHY CREATE A REPORTING AND ESCALATION POLICY?

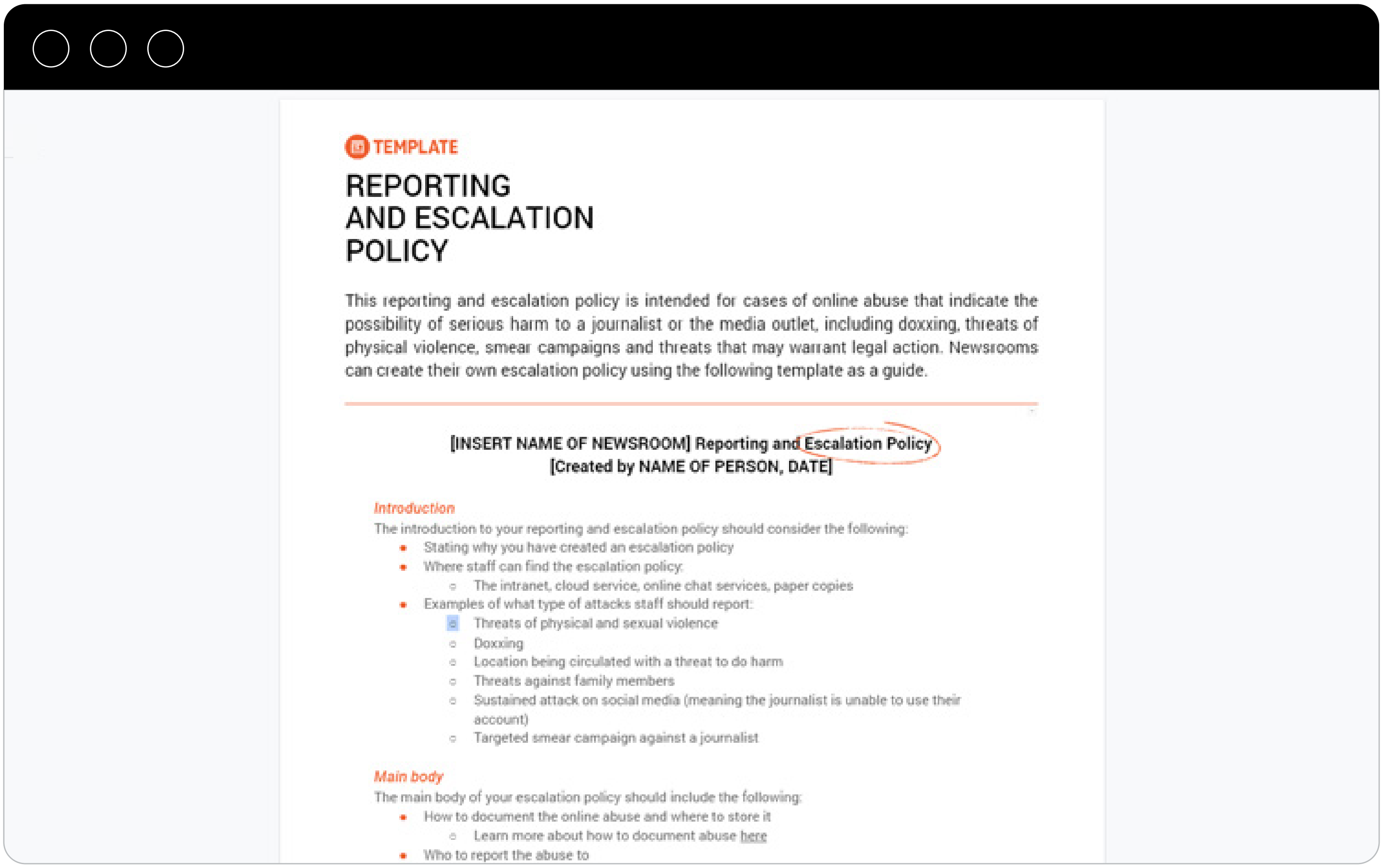
Reporting and escalation policies give clarity to both managers and journalists on what to do and who to speak to should there be a serious incident of online harassment. The policy should state clearly what types of abuse a journalist should report, who to report the abuse to and what will happen once it has been reported.

# WHAT TO CONSIDER WHEN CREATING A REPORTING AND ESCALATION POLICY

- An escalation policy should be part of a wider package of support for staff targeted by online abuse, including informal check-ins, speaking openly about online abuse and its effect on staff and the creation of an online space, such as Slack or WhatsApp, where staff can discuss issues related to online harassment.
- An escalation policy is designed to tackle harassment, which could indicate a serious threat to the journalist or newsroom. This could include doxxing, threats of physical violence, targeted smear campaigns and threats that could warrant legal action.
- Management should be mindful that online abuse disproportionately affects women and diverse journalists, and that they may be hesitant to report abuse.
- For a reporting and escalation policy to be effective, it's important to have buy-in and support from all staff involved in the process, including training on what to do if they receive a report of abuse, how to speak with staff members about the abuse they have received and how to let staff know about next steps.
- Inform staff about the reporting and escalation policy and let them know when, how and who they should report to.
- It's important that staff who report incidents of abuse feel included in the process. Decisions, such as reporting abuse to the authorities, should not be taken without their permission.

# REPORTING AND ESCALATION POLICY

This reporting and escalation policy is intended for cases of online abuse that indicate the possibility of serious harm to a journalist or the media outlet, including doxxing, threats of physical violence, smear campaigns and threats that may warrant legal action. Newsrooms can create their own escalation policy using the following template as a guide. You can access an online version of this form **here**



TEMPLATE

REPORTING AND ESCALATION POLICY

This reporting and escalation policy is intended for cases of online abuse that indicate the possibility of serious harm to a journalist or the media outlet, including doxxing, threats of physical violence, smear campaigns and threats that may warrant legal action. Newsrooms can create their own escalation policy using the following template as a guide.

**[INSERT NAME OF NEWSROOM] Reporting and Escalation Policy**
**[Created by NAME OF PERSON, DATE]**

*Introduction*

The introduction to your reporting and escalation policy should consider the following:

- Stating why you have created an escalation policy
- Where staff can find the escalation policy:
  - The intranet, cloud service, online chat services, paper copies
- Examples of what type of attacks staff should report:
  - Threats of physical and sexual violence
  - Doxxing
  - Location being circulated with a threat to do harm
  - Threats against family members
  - Sustained attack on social media (meaning the journalist is unable to use their account)
  - Targeted smear campaign against a journalist

*Main body*

The main body of your escalation policy should include the following:

- How to document the online abuse and where to store it
  - Learn more about how to document abuse here
- Who to report the abuse to

CASE STUDY

# CREATING A REPORTING AND ESCALATION POLICY

Protocol reached out to us for support after a staff member was targeted online because of their work covering China. The outlet wanted help putting together a number of policies that would help better protect staff. One of the areas we focused on was creating an escalation policy for the newsroom.

## PROTOCOL

### ABOUT THE NEWSROOM

Number of journalists in the newsroom:
**50**

Location:
**Distributed team with journalists predominantly in the USA**

Type of newsroom:
**Online publication covering the technology industry**

## HISTORY OF ONLINE ATTACKS

Journalists working at the newsroom receive attacks on social media and via email, especially after publishing on certain stories. The attacks include hateful comments and harassment. The outlet wanted to provide staff with processes, tools and training to help them deal with these issues of abuse.

## OUR SUPPORT

We worked with the Executive Editor and the Head of People Operations and Chief of Staff at Protocol to design a guide that would be practical to use with a distributed team. Part of the guide included the creation of a reporting and escalation policy for staff wanting to report online abuse. We worked with the team to establish which departments in the newsroom should be involved in the escalation policy as well as helping them think through what additional support could be provided for their staff, including counseling and sessions with physical and digital security experts.

## WHAT HAPPENED NEXT

Protocol made its policy available to staff and is currently putting its reporting and escalation policy to use. The guidelines enabled reporters to escalate problems to their editors and HR leading to attacks being dealt with more quickly and effectively.

> "The policies that the IWMF helped us to create were valuable in creating more transparency when a staff member is facing an online attack, and it also gave them a framework to use when escalating issues."
>
> *Maria Harrigan, Chief of Staff, Protocol*

CHAPTER 7

# STATEMENTS OF SUPPORT, CLARIFICATION, AND FAQ

# WHY CREATE STATEMENTS OF SUPPORT, STATEMENTS OF CLARIFICATION AND/OR AN FAQ?

Online harassers can use sophisticated smear campaigns against a journalist or a media outlet as a way to undermine their credibility. Smear campaigns can be relentless and lengthy, and include tactics such as digging up and misrepresenting old social media posts as a way to discredit a reporter. For media outlets, smear campaigns often target their sources of funding as a way to question their impartiality and to try to damage their reputation with readers.

Journalists who are targeted by well-orchestrated smear campaigns benefit from the support of their media outlet and their peers. Creating a statement of support clarifies the situation for readers but it also sends a message to staff that the media outlet is behind them. A media outlet that is targeted by a one-off smear campaign can issue a statement of clarification addressing the situation. If a newsroom is constantly targeted by smear campaigns, then creating an FAQ addressing issues such as funding sources may be a good option.

# WHAT TO CONSIDER WHEN CREATING STATEMENTS OF SUPPORT, STATEMENTS OF CLARIFICATION AND/OR AN FAQ

## STATEMENTS OF SUPPORT

- Procedures on what to do if targeted by a smear campaign should be included in the newsroom's escalation policy.

- The media outlet should make its policy on smear campaigns clear to staff. These guidelines should include information on whether statements of support will be issued, in what circumstances and the procedure for issuing the statement.

- The journalist should always be included in the drafting of a statement of support.

- A statement of support may include the following information, an overview of the situation, the newsroom's position with regards to the harassment.

- Both the journalist and the newsroom should be aware that there may be an increase in online harassment as a result of the statement being issued. The newsroom should work with the journalist to ensure their online data and their accounts are as secure as possible before issuing the statement.

- Statements of support can be pinned to the top of the individual journalist's social media feeds.

- Once a statement of support is issued, it is recommended that neither the journalist nor the outlet engage further with the harassers.

## STATEMENTS OF CLARIFICATION AND FAQ

- The media outlet should have clear guidelines for when to issue a statement of clarification. Relevant departments should be included in the drafting of the clarification.

- The newsroom should be aware that issuing a statement of clarification could lead to increased levels of harassment.

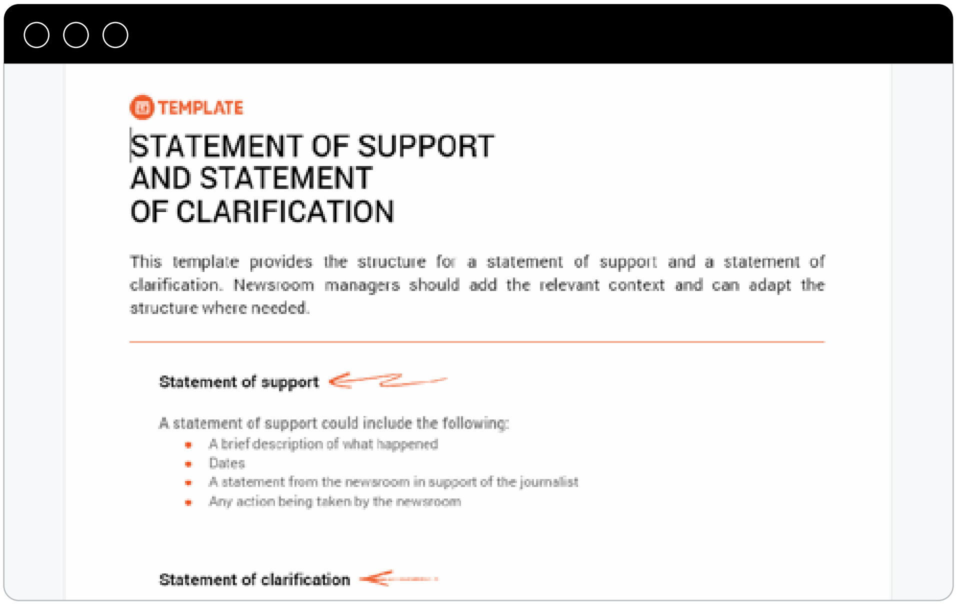
- Before issuing a statement of clarification the newsroom should speak with its IT department to ensure that the highest level of security is activated for staff accounts and for the website.

- An FAQ should address common questions that readers may have about the newsroom.

- An FAQ can be included as a permanent feature on the outlet's website.

# STATEMENT OF SUPPORT AND STATEMENT OF CLARIFICATION

This template provides the structure for a statement of support and a statement of clarification. Newsroom managers should add the relevant context and can adapt the structure where needed. An online version of this structure can be found **here**



TEMPLATE

STATEMENT OF SUPPORT AND STATEMENT OF CLARIFICATION

This template provides the structure for a statement of support and a statement of clarification. Newsroom managers should add the relevant context and can adapt the structure where needed.

**Statement of support**

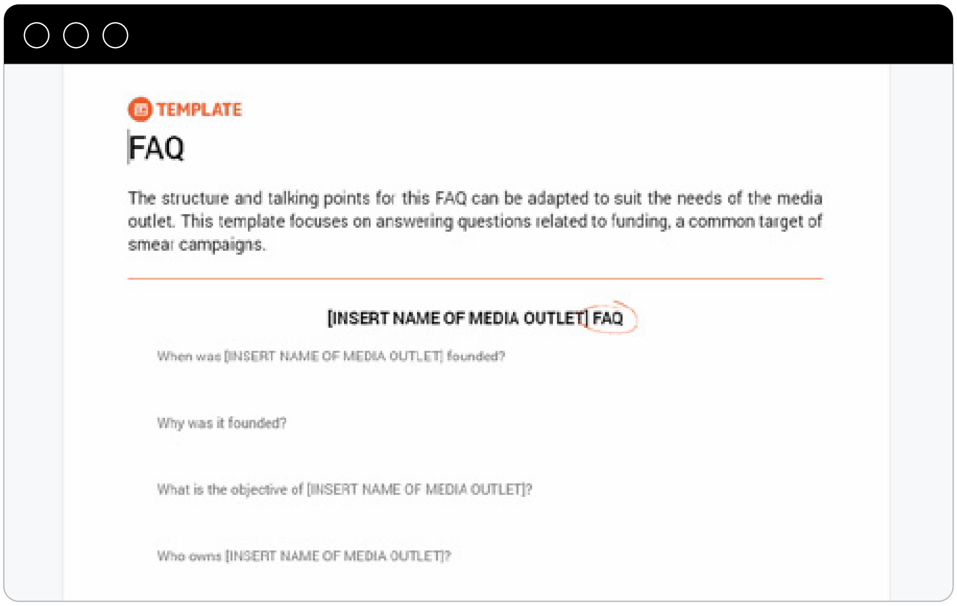
A statement of support could include the following:

- A brief description of what happened
- Dates
- A statement from the newsroom in support of the journalist
- Any action being taken by the newsroom

**Statement of clarification**

# FAQ

The structure and talking points for this FAQ can be adapted to suit the needs of the media outlet. This template focuses on answering questions related to funding, a common target of smear campaigns. You can access an online version of this form **here**



TEMPLATE

FAQ

The structure and talking points for this FAQ can be adapted to suit the needs of the media outlet. This template focuses on answering questions related to funding, a common target of smear campaigns.

**[INSERT NAME OF MEDIA OUTLET] FAQ**

When was [INSERT NAME OF MEDIA OUTLET] founded?

Why was it founded?

What is the objective of [INSERT NAME OF MEDIA OUTLET]?

Who owns [INSERT NAME OF MEDIA OUTLET]?

CHAPTER 8

# ONLINE VIOLENCE GUIDE FOR THE NEWSROOM

# WHY CREATE AN ONLINE VIOLENCE GUIDE?

An online abuse guide allows a newsroom to present all of its online abuse policies in one place. The content of the guide can be adapted to the needs of the newsroom and can include sections such as defining online abuse, account security and an escalation policy, amongst others. The guide should be easy to read and located in a place that staff can find.

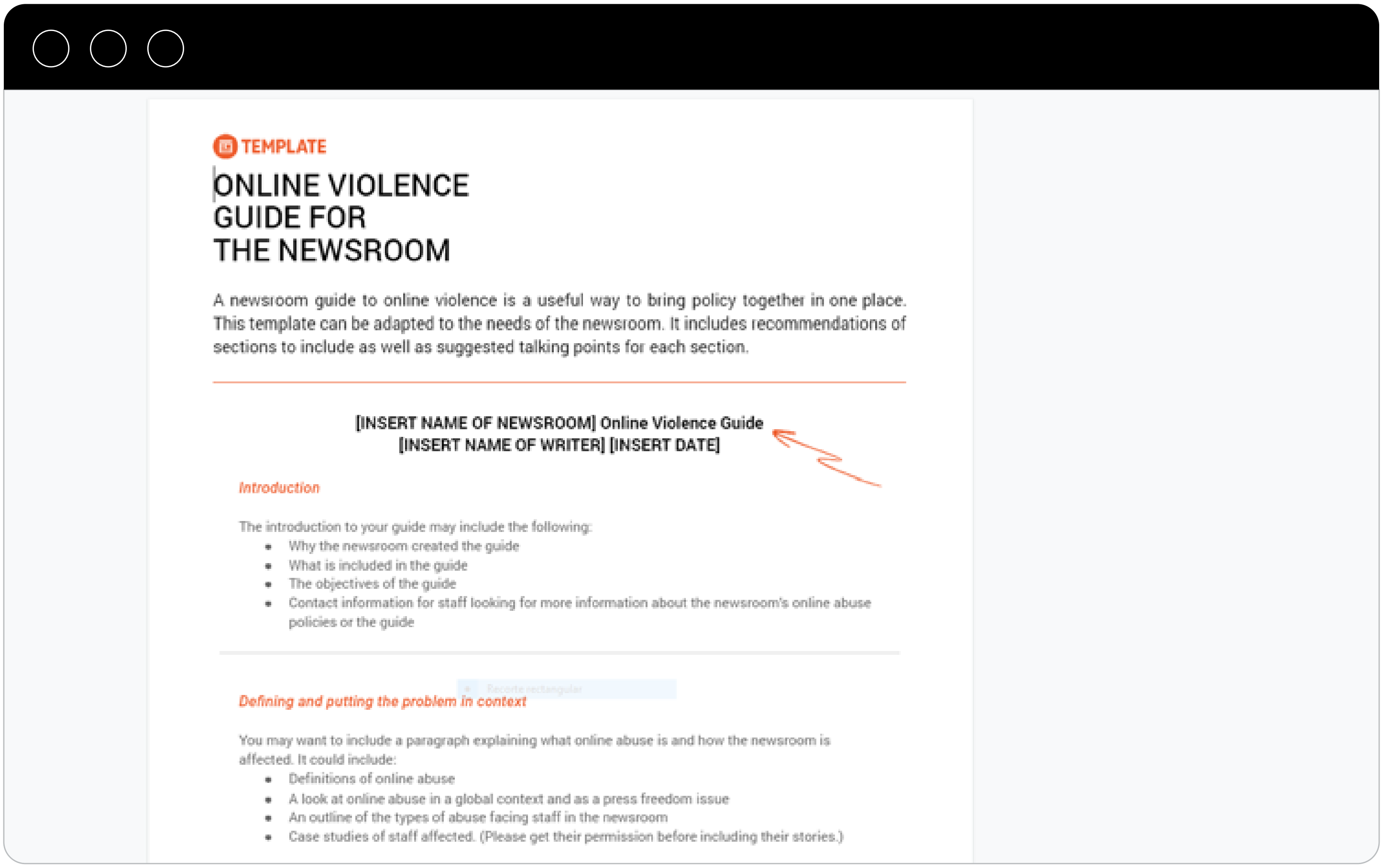
# WHAT TO CONSIDER WHEN CREATING YOUR GUIDE

- Each newsroom has different needs and wants when it comes to creating online abuse policies. Choose policies that will be possible to implement and that will help increase staff safety.
- The guide should be written with your staff in mind and should be written in clear language with no jargon.
- The guide should acknowledge that online abuse happens to staff in the newsroom.
- The guide can be accompanied by other support for staff, such as a survey or a statement of support. These do not have to be included in the guide for staff.
- Staff should be informed about the guide and where to find it. For example, it can be placed on the staff intranet or pinned to the top of online communications channels, such as Slack. You may want to leave paper copies in the office.
- The guide should include the date it was created and be reviewed periodically to make sure the guidance is up to date.

TEMPLATE

# ONLINE VIOLENCE GUIDE FOR THE NEWSROOM

A newsroom guide to online abuse is a useful way to bring policy together in one place. This template can be adapted to the needs of the newsroom. It includes recommendations of sections to include as well as suggested talking points for each section. You can access an online version of this form here



TEMPLATE

## ONLINE VIOLENCE GUIDE FOR THE NEWSROOM

A newsroom guide to online violence is a useful way to bring policy together in one place. This template can be adapted to the needs of the newsroom. It includes recommendations of sections to include as well as suggested talking points for each section.

**[INSERT NAME OF NEWSROOM] Online Violence Guide**
**[INSERT NAME OF WRITER] [INSERT DATE]**

*Introduction*

The introduction to your guide may include the following:

- Why the newsroom created the guide
- What is included in the guide
- The objectives of the guide
- Contact information for staff looking for more information about the newsroom's online abuse policies or the guide

*Defining and putting the problem in context*

You may want to include a paragraph explaining what online abuse is and how the newsroom is affected. It could include:

- Definitions of online abuse
- A look at online abuse in a global context and as a press freedom issue
- An outline of the types of abuse facing staff in the newsroom
- Case studies of staff affected. (Please get their permission before including their stories.)

CASE STUDY

# ONLINE VIOLENCE GUIDE FOR THE NEWSROOM

The Seattle Times was the first outlet to reach out to the IWMF for help in creating online abuse policies. They wanted to increase awareness of online harassment within the newsroom as well as develop policies and best practices to better protect staff. We supported The Seattle Times with the creation of an online abuse guide, which the newsroom made open source so that other outlets could benefit from what they learned.

## THE SEATTLE TIMES

### ABOUT THE NEWSROOM

Number of journalists in the newsroom:
**170**

Location:
**Seattle, U.S.**

Type of newsroom:
**The Seattle Times is a 125-year-old independent and locally owned new media company**

## HISTORY OF ONLINE ATTACKS

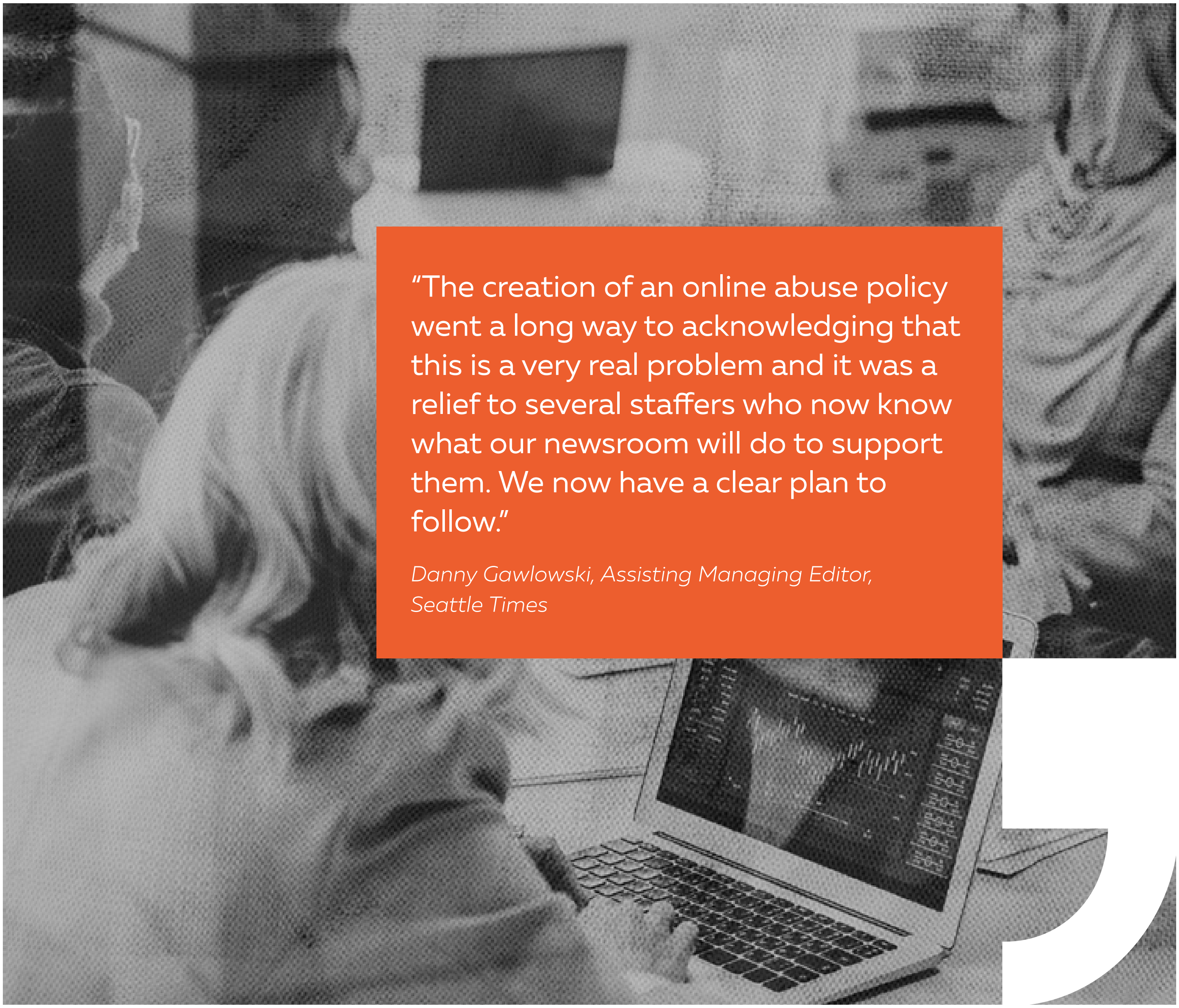
Journalists at The Seattle Times, particularly women and Black, Indigenous and people of color (BIPOC) journalists receive regular harassment through email and social media. Threats of physical violence have also been used against the staff and the newsroom as a whole. The Seattle Times also receives regular hacking attacks on the site's infrastructure and several staffers had their social media accounts hacked.

## OUR SUPPORT

We worked with the Assistant Managing Editor for Diversity, Inclusion and Staff Development and the Assistant Managing Editor to design a roundtable for management and HR leadership teams aimed at creating greater awareness of issues linked to online abuse in the newsroom. This session included collaboration with Freedom of the Press Foundation. We then worked for several months to support the newsroom with creating an online abuse guide for staff. The guide included an overview of what online abuse is as well as guidance for staff on how to secure their online data and their accounts. The guide also included an escalation policy with clear roles and duties around responding to severe threats. Collaboration between newsroom leadership, IT and HR was an important part of ensuring the success of the guide.

## WHAT HAPPENED NEXT

The Seattle Times shared its guide with staff and ensured that it was located in a place that staff could locate easily. It decided to make the guide open source so that other newsrooms could benefit from what The Seattle Times created. Newsroom leaders also wrote an article for Better News about their experience creating the guide and what they learned. You can read about their experiences **here** and get inspiration for your own guide **here**.



> "The creation of an online abuse policy went a long way to acknowledging that this is a very real problem and it was a relief to several staffers who now know what our newsroom will do to support them. We now have a clear plan to follow."
>
> *Danny Gawlowski, Assisting Managing Editor, Seattle Times*

# SUGGESTED RESOURCES

The following resources have been created by members of the Coalition Against Online Violence. They are reviewed regularly to ensure they are up to date.

| | |
|---|---|
| ACCOUNT SECURITY | The Coalition Against Online Violence<br>Account security |
| DOCUMENTING ABUSE | Online SOS<br>Proper Documentation |
| MENTAL HEALTH AND WELLBEING | The Coalition Against Online Violence<br>Psychosocial support |
| | International Press Institute<br>Risk of emotional impact on the journalist |
| ONLINE ABUSE SURVEY | International Press Institute<br>Staff survey |
| REPORTING AND ESCALATION | International Press Institute<br>Reporting form |
| RISK ASSESSMENT | Committee to Protect Journalists<br>Editor's checklist: Protecting staff and freelancers against online abuse |
| UNDERSTANDING ONLINE HARASSMENT | Coalition Against Online Violence<br>Learn more about online violence |
| | PEN America<br>Defining online abuse: a glossary of terms |
| | Right to Be<br>Understanding online harassment |

# A GUIDE TO PROTECTING NEWSROOMS AND JOURNALISTS AGAINST ONLINE VIOLENCE

INTERNATIONAL WOMEN'S MEDIA FOUNDATION