



Journalist Fellowship Paper

# Keeping journalists safe online: a guide for newsrooms in West Africa & beyond

By **Gideon Sarpong**

April 2022

Hilary Term

Sponsor: Fondation Botnar



# Contents

Introduction	3
Build digital rights literacy	6
Defining online abuse and harassment	6
Training and awareness creation	8
Knowledge sharing	10
Additional tools and resources	10
Establish safety practices	11
Adapt the newsroom culture	11
Maintain clear reporting lines and channels	12
Keep records of online attacks and harassment	13
Complete a risk analysis	14
Risk of physical harm	14
Risk of psychological harm	14
Risk of reputational harm	15
Additional tools and resources	15
Implement support mechanisms	16
Digital security support	16
Legal support	16
Emotional and psychological support	17
Temporary leave, relocation, and/or reassignment	18
Public statement of support	18
Moderating online content	19
Security Training	21
Additional tools and resources	22
Assign roles and tasks	24
Online safety coordinator	24
Management	25
Editors	25
Moderators	25
Journalists	26
Acknowledgements	27

# Introduction

Social media platforms have given journalists many opportunities – facilitating the exchange of views and information, promoting their content, and improving audience engagement – but they’ve also created new threats to safety and wellbeing, particularly for women journalists.

As noted in the [RSF 2020 Index](#), social media has generated prolific online harassment and abuse for journalists across Africa reporting on contested social, economic and political issues.<sup>1</sup> These online threats include targeted smear campaigns that erode the foundations of journalism by chipping away at journalists’ resolve to provide independent, critical reporting on crucial issues.

In 2020, UNESCO and the International Center for Journalists (ICFJ) conducted a [survey](#) on online violence against women journalists in 15 countries, including Ghana and Nigeria.<sup>2</sup> They found that 73% of those who participated in the survey had experienced online violence, with Facebook and Twitter ranked among the least safe platforms for women journalists.

Award-winning Nigerian journalist Ruona Meyer is among the victims of such attacks. She was targeted in a campaign of [extreme online harassment](#)<sup>3</sup> which lasted almost a year following publication of her BBC investigation into [Nigeria’s cough syrup cartels](#).<sup>4</sup> “Whenever they want to turn the Nigerian public against me they’ll

---

<sup>1</sup> RSF. 2022. 2020 RSF Index: Future of African journalism under threat from all sides. [online] Available at: <<https://rsf.org/en/2020-rsf-index-future-african-journalism-under-threat-all-sides>> [Accessed 22 February 2022].

<sup>2</sup> Unesdoc.unesco.org. 2022. [online] Available at: <<https://unesdoc.unesco.org/ark:/48223/pf0000375136>> [Accessed 22 February 2022].

<sup>3</sup> En.unesco.org. 2022. [online] Available at: <<https://en.unesco.org/sites/default/files/the-chilling.pdf>> [Accessed 22 February 2022].

<sup>4</sup> BBC News. 2022. The codeine investigation that changed Nigeria. [online] Available at: <<https://www.bbc.co.uk/news/av/world-africa-48532120>> [Accessed 22 February 2022].

say things like I'm wayward, I married a foreigner...," she told UNESCO. "What has that got to do with my work as a journalist?"

[iWatch Africa](#) also tracked over 5,000 cases of online abuse and harassment directed at journalists in Ghana in 2020.<sup>5</sup> These incidents are a representation of what happens in other countries across the continent, sometimes leading to physical harm. In 2017, the Committee to Protect Journalists found that in [at least 40% of cases](#), journalists who were murdered had received threats, including online threats, before they were killed.<sup>6</sup>

The [UNESCO survey](#) also found that many women journalists have had to deal with mental health issues as a result of online harassment, and many others have resorted to self-censorship, complete withdrawal from all social media interaction, and avoidance of audience engagement.

The guidelines contained here specify steps and measures that newsrooms and journalists in West Africa can take to mitigate the problem of online abuse.

The purpose is not to shield journalists from criticism or promote the criminalization of online speech, but to deal with a real threat facing journalism today, which has the potential to erode press freedom in West Africa if it goes unchecked.

---

<sup>5</sup> iWatch Africa. 2022. Q2 Report: Manasseh Azure, Nana Aba Anamoah & Justice Annan among most abused journalists online - iWatch Africa. [online] Available at: <<https://iwatchafrica.org/2020/07/27/q2-report-manasseh-azure-nana-aba-anamoah-justice-annan-among-most-abused-journalists-online/>> [Accessed 22 February 2022].

<sup>6</sup> Committee to Protect Journalists. 2022. Getting Away with Murder - Committee to Protect Journalists. [online] Available at: <<https://cpj.org/reports/2017/10/impunity-index-getting-away-with-murder-killed-justice-2/>> [Accessed 22 February 2022].

Modelled after research published by [UNESCO](#)<sup>7</sup> and the [International Press Institute](#),<sup>8</sup> this guide is specifically tailored to meet the unique demands and resource constraints facing newsrooms in West Africa.

It is not intended to be a one-size-fits-all set of protocols; it should be adapted and modified to fit the needs of individual newsrooms. In the long run, these guidelines will require constant reassessment and updating to accommodate rapid changes in technology, social media tools, and the political landscape that informs online attacks.

The roadmap outlined on the following pages includes five action points:

1. Build digital rights literacy
2. Establish safety practices
3. Complete a risk analysis
4. Implement support mechanisms
5. Assign roles and tasks

Throughout the guide, I have also incorporated additional tools and resources to serve as key reference points for freelance journalists who may need extra support in fending off online threats and harassment.

The risks that online harassment poses to the free flow of information, press freedom, and the democratic exchange of ideas demand an urgent response.

---

<sup>7</sup> En.unesco.org. 2022. [online] Available at: <<https://en.unesco.org/sites/default/files/the-chilling.pdf>> [Accessed 22 February 2022].

<sup>8</sup> Ipi.media. 2022. [online] Available at: <<https://ipi.media/wp-content/uploads/2019/06/IPI-report-online-harassment-06032019.pdf>> [Accessed 22 February 2022].

# Build digital rights literacy

In the online era, digital rights have become akin to human rights. This was affirmed by [Resolution 362 on the Right to Freedom of Information and Expression on the Internet in Africa](#) passed by the African Commission on Human and Peoples' Rights.<sup>9</sup> Digital rights protect citizens' equal opportunity to exercise their freedom of expression and access information online without discrimination.

## Defining online abuse and harassment

Online abuse and harassment manifests in various forms and can encompass a huge range of attacks on the internet, including on major social media platforms, or through the use of specific apps or technologies.

Many of them are gender-based attacks targeting women journalists in response to their journalistic activities with the purposes of threatening, intimidating and silencing them.

The most significant forms of abuse journalists encounter fall under the following categories as defined by [Article 19](#).<sup>10</sup>

### Doxxing

This involves the public dissemination of a journalist's personal information, such as email, telephone or home address. This can often result in increased harassment, and create a safety risk.

### Surveillance

Whether perpetrated by public or private entities, this involves monitoring of a journalist's online and/or offline life through technological means.

---

<sup>9</sup> PLC, A., 2022. African Commission on Human and Peoples' Rights Sessions. [online] Achpr.org. Available at: <<https://www.achpr.org/sessions/resolutions?id=374>> [Accessed 14 January 2022].

<sup>10</sup> ARTICLE 19. 2022. Online abuse and harassment against women journalists - ARTICLE 19. [online] Available at: <<https://www.article19.org/onlineharassment/>> [Accessed 14 March 2022].

## Threats

These are targeted through digital platforms or apps, and often include threats of physical or sexual violence.

## Harassment

Like offline harassment, this can include a range of unwanted and intimidating activities including contact through messages or apps. Online, this can often take the form of “pile-ons”, with multiple perpetrators.

## Non-consensual distribution of intimate or sexual images

This refers to the sharing of sexual or intimate images of a journalist, which can be taken with (or by him/her) or without their knowledge, and either by someone who has access to them with consent (but there is no consent for them to be further shared), or by someone who gains access through other means. This can have serious psychological and reputational consequences.

## Hacking

This is when someone gains access to a journalist’s private accounts or devices through malicious means. This can often lead to another form of attack, including blackmail.

## Identity theft or unauthorised use of accounts

Where someone is able to take control of or in some way impersonate a journalist’s online presence.

## Discriminatory and sexist speech and gender stereotypes

This can include a wide range of types of speech based on negative stereotypes or on the basis of a woman’s gender, nationality, religious belief, race, among others.

This list is not an exhaustive one and should be regularly updated to reflect newer abuses and harassment.

To effectively counter online abuse and harassment, the promotion of digital literacy in newsrooms is key. Understanding issues related to digital rights is an important step in addressing the psychological, physical, and digital safety impacts associated with this new “frontline of attack”, as ICIJ describes it.<sup>11</sup>

Training is also important in helping journalists participate in discussions and debates for policy development and change, so that they understand how human rights apply online, and are aware when their rights have been violated.

For the purposes of this guide, digital rights literacy focuses on ensuring journalist’s understand the [Charter of Human Rights and Principles for the Internet](#), a set of 10 internet governance principles rooted in international human rights standards.<sup>12</sup> To paraphrase, these include the expectation of equality, justice, accessibility, free expression and association, a fair expectation of privacy and data protection, a right to secure life and liberty, diverse representation, network (structural) equality, open standards and regulation, and transparent governance.

### Training and awareness creation

Newsroom managers should initiate digital rights literacy programmes that are inclusive and gender sensitive to ensure that there is equal access to opportunities and resources for people who might otherwise be excluded or marginalised based on gender or sexual orientation.

---

<sup>11</sup> International Center for Journalists. 2022. Online Violence: The New Front Line for Women Journalists\*. [online] Available at: <<https://www.icfj.org/news/online-violence-new-front-line-women-journalists>> [Accessed 14 February 2022].

<sup>12</sup> Internet Rights and Principles Coalition. 2022. 10 Internet Rights & Principles – Internet Rights and Principles Coalition. [online] Available at: <<https://internetrightsandprinciples.org/campaign/>> [Accessed 14 January 2022].

## Adopt, adapt, and share training resources

- Adapt existing resources to create a simple training module for journalists in the organisation. The Media Legal Defence Initiative (MLDI) has a comprehensive [training module](#) that can help you design a training programme for journalists.<sup>15</sup>
- Use an existing online course or training manual. Some, like MLDI's module, are already available for free online. This will allow journalists to easily share training material with their peers and spread the word. Putting your training course or informational material online will also save you some resources, like venue and travel costs.
- Record any face-to-face training you conduct, and make them available on an online platform.
- Consider making the course multilingual, especially if you are working in a location with multiple language groups.

## In-person interventions

Holding in-person meet-ups with journalists can be the most effective way to track new developments, build community, and share resources. These could take the form of:

- **Formal meetings:** Establish regular lectures on digital rights and an open forum where journalists can ask questions and share their ideas on how digital rights are (or are not) being applied in the online space.
- **Informal meetings:** Set up nontraditional events, such as tea or coffee gatherings, with journalists.

---

<sup>15</sup> Mediadefence.org. 2022. [online] Available at: <<https://www.mediadefence.org/wp-content/uploads/2020/06/MLDI-Training-Manual-on-Digital-Rights-and-Freedom-of-Expression-Online.pdf>> [Accessed 14 January 2022].

## Knowledge sharing

- Create accessible and easy-to-understand content that takes all journalists' needs into account. Consider making content available in different formats, like videos, podcasts, posters, or manuals.
- Create a method for continuous engagement, such as a Signal or email group. This will enable journalists to continue to discuss, report, and exchange relevant information on digital rights issues.
- Post engaging content on digital rights to your online community.

## Additional tools and resources

### Training materials and platforms

- [Multimedia training kit on human rights and the internet](#)<sup>14</sup>
- The Democratic Principles for an Open Internet ([videos](#))<sup>15</sup>
- [Open edX](#) offers the option to customise its online learning platform either through a service provider or a self-service deployment (requires more technical knowledge and resources).<sup>16</sup>

### Policy resources

International Frameworks and Conventions on Human Rights in the Digital Space has issued the [African Declaration on Internet Rights and Freedoms](#)<sup>17</sup>

---

<sup>14</sup> Apc.org. 2022. 'Human rights and the internet' multimedia training kit released | Association for Progressive Communications. [online] Available at: <<https://www.apc.org/en/news/human-rights-and-internet-multimedia-training-kit>> [Accessed 14 January 2022].

<sup>15</sup> Youtube.com. 2022. Before you continue to YouTube. [online] Available at: <<https://www.youtube.com/channel/UCOPYRyVkdeWEicoheD4Wfbw/videos>> [Accessed 14 January 2022].

<sup>16</sup> Open.edx.org. 2022. Open edX – Deliver Inspiring Learning Experiences On Any Scale. [online] Available at: <<https://open.edx.org/>> [Accessed 14 January 2022].

<sup>17</sup> Africaninternetrights.org. 2022. African Declaration on Internet Rights and Freedoms. [online] Available at: <<https://africaninternetrights.org/>> [Accessed 14 January 2022].

# Establish safety practices

## Adapt the newsroom culture

Send an email to all staff making it clear that the media organisation takes online violence and abuse very seriously. This measure is an important first step for building confidence in the newsroom.

It sends two important messages: First, it helps debunk the widespread feeling among journalists that being targeted with abuse on social media is the new normal; and second, it gives journalists a sense of security that the media organisation will support them.

The email should emphasise the following to maximise impact:

- A commitment from the organisation to take online threats and harassment seriously, and that journalists are encouraged to report it.
- Make clear that seeking support in the case of online harassment is not shameful and that journalists do not need to be so “tough” that they decline to report serious threats against them.
- Information about tools the company has in place to support journalists targeted and how journalists can report instances of threats and harassment. (See sections on support mechanisms, and roles and tasks.)

Next, establish regular meetings between social media teams and journalists to carry out a “health check” related to journalists’ work on social media or engagement in online comment sections.

Finally, newsroom managers and editors should keep written company policies on online harassment visible and accessible. They should also ensure that employees

are familiar with the tools and protocols the company has created to deal with the issue (e.g. posters in newsrooms).

### Maintain clear reporting lines and channels

All staff members and contributors should know who to report abuse to and how to report it. Newsrooms should create various channels through which attacks can be easily reported and that allow journalists to access support mechanisms.

These might include:

- Informal reporting mechanism: Encourage informal talks with colleagues. Newsrooms should encourage journalists to share experiences of harassment with their peers and editors. Journalists should be encouraged to use chat groups to report online abuse.
- Formal reporting mechanisms: Formal reporting mechanisms create an expectation of action. Therefore, it must be made clear to journalists and other staff members who is responsible for receiving the reports and what steps that person can take.
- Create an online form where targeted journalists can easily report an online attack. The form should be short and easy to fill in, but cover all essential information related to the attack.
- Create a specific email address where journalists can report online harassment.

Newsrooms should ensure that coordinators of reporting mechanisms include representation from women and minorities. They should also make sure that all coordinators have been made sensitive to the specific types of attacks targeting women and minorities.

## Keep records of online attacks and harassment

Create a database to keep track of reported incidents of online harassment, as well as information about the responses taken. This could be as simple as using a [Google form](#) to store submissions and responses.<sup>18</sup>

Take screenshots of abuses. Include as much information as possible in the screenshot, including shares and likes, and date/time/location information that is sometimes shown below a post.

Label and store the screenshots in a clear folder structure so that they can be easily retrieved and identified. For example:

My Drive > Online harassment records > January 2022 ▾

Name	Owner
 Journalist Name_Reddit_2022-01-24 at 15.24.41.png	me
 Journalist Name_Twitter_2022-01-25 at 10.22.27.png	me
 Journalist Name_Facebook_2022-01-25 at 10.24.20.png	me
 Journalist Name_Twitter_2022-01-25 at 14.30.16.png	me

*A folder structure on Google Drive, where screenshots of harassment are gathered in folders based on month the abuse was received, and labelled to include the name of the journalist involved, the platform the abuse was received on, and the date the screengrab was taken*

<sup>18</sup> Google.co.uk. 2022. Google Forms: Free Online Form Creator | Google Workspace. [online] Available at: <<https://www.google.co.uk/forms/about/>> [Accessed 14 January 2022].

# Complete a risk analysis

In the event of an online attack, conducting a thorough assessment of risks – including physical, psychological and reputational harms – is important to determine which type of support is most appropriate.

## Risk of physical harm

Factors to consider include:

- Overall online environment in your country (e.g. history and frequency of online attacks leading to physical attacks on the press, impunity for such attacks, climate of generalised animosity toward the press).
- In the case of an individual aggressor, assessment of risk of physical attack based on known information about this individual.
- In the case of campaigns, likelihood that individuals will feel encouraged or legitimised to carry out a physical attack.
- The public nature of the journalist's work: how recognizable is he or she in public places?

## Risk of psychological harm

Factors to consider include:

- Intensity of the harassment, both in content and frequency.
- Inclusion of discriminatory character-based content (e.g. is it based on gender, race, sexual orientation), which can have a particularly serious impact on the target.
- Presence of traumatic imagery.
- Messages that indicate stalking behaviour, which can generate fear and insecurity.
- Strength of the target's overall support network.
- Target's psychological state (signs of depression or trauma).

## Risk of reputational harm

Factors to consider include:

- Degree of polarisation and hostility toward media present in society.
- Potential for the smears to be considered credible by the public.
- Volume and reach of attacks and smear campaigns, including factors that can allow online attacks to spread more quickly, such as attacks using memes or elaborate graphic designs, botnets, and labels; and smears that have the potential to be recycled in the future.
- An indication that smear campaigns have been orchestrated on behalf of political, economic, or other interests.

## Additional tools and resources

- The Global Investigative Journalism Network (GIJN) has created a self-assessment [safety evaluation guide](#) for watchdog journalism groups.<sup>19</sup>
- In West Africa, the [Media Foundation for West Africa](#) provides support to journalists who face extreme dangers as a result of their work.<sup>20</sup>
- [Free Press Unlimited](#) also provides support for journalists who face intense harassment online.<sup>21</sup>

---

<sup>19</sup> Philp, R., 2022. GIJN Launches Journalism Security Assessment Tool. [online] Global Investigative Journalism Network. Available at: <<https://gijn.org/2021/11/02/gijn-launches-journalism-security-assessment-tool/>> [Accessed 14 February 2022].

<sup>20</sup> Media Foundation For West Africa. 2022. Home - Media Foundation For West Africa. [online] Available at: <<https://www.mfwa.org/>> [Accessed 14 February 2022].

<sup>21</sup> Free Press Unlimited. 2022. Reporters Respond: emergency & legal support. [online] Available at: <<https://www.freepressunlimited.org/en/projects/reporters-respond-emergency-and-legal-support>> [Accessed 14 February 2022].

# Implement support mechanisms

These support mechanisms help ensure that journalists can do their work without fear of harm or abuse.

## Digital security support

Minimise the potential harm of online attacks by:

- Blocking the users behind attacks, even if they have posted the threats from anonymous accounts on social media.
- Lock down all of the target's accounts by changing their passwords to protect against hackers and/or consider adding temporary restrictions to who can access or comment on posts.
- The newsroom manager may offer to take over the target's social media accounts so that the target is not exposed to further abuse.

Take preventive measures:

- Make journalists aware of what personal details are accessible to the public through their social media accounts. See if any sensitive information has been exposed unintentionally.
- Train journalists to scan their electronic devices to identify potential vulnerabilities that might allow hackers to access their personal data and publicly expose it. Teach them to spot phishing scams.

## Legal support

Factors to consider before legal action is taken:

- Whether the post contains illegal content according to your local laws.
- The likelihood that bringing a case will deter future online aggressors in general.
- The likelihood that bringing a case will deter the actions of the specific aggressor in this case.

- The possibility that, given the particular context, pursuing legal action will spotlight the particular journalist and amplify and encourage further attacks.
- Whether legal action could unwittingly reinforce stories that online aggressors may already be selling about “powerful” media organisations attacking the “little guy” – potentially fueling further harassment.
- Whether the attack appears to have been perpetrated by an individual acting alone or someone participating in a coordinated campaign. In the latter case, legal action may be counterproductive and provoke further attacks.
- The potential impact on the journalist affected. Will a legal case bring satisfaction to the affected journalist, or will it cause further emotional harm?
- Whether prosecutors have also taken up a criminal case, in which case it may be easier to support that effort.

### Emotional and psychological support

Offering professional mental health support can play an important role in helping mitigate the consequences of online abuse and harassment of journalists. Because this form of support could place additional financial burden on newsrooms in West Africa, a list of organisations that offer free support has been included at the end of this section. (See *Additional tools and resources*, pg 22.)

Peer support is another viable option: For journalists targeted with online abuse and harassment, colleagues who have endured similar experiences can be an important source of strength, empathy, and knowledge of how best to cope with the attacks and their potential consequences.

Develop a formal network of staff members in the newsroom who are available to listen to the experiences of their peers who have been targeted with online abuse and walk them through ways of coping with the effects.

Consider implementing mentoring programmes:

- Assign a senior journalist to mentor less-experienced colleagues.
- Mentors should help mentees recognise online abuse, the topics that typically lead to it, and the forms that it may take.

A chat group using an encrypted messaging app like Signal or a similar app can be used not only to report threats, but also to provide support in case of attacks.

Editors should be encouraged to create opportunities to discuss the issue of online harassment in group settings.

### Temporary leave, relocation, and/or reassignment

Based on your assessment of the emotional distress of the targeted journalist, a brief temporary leave can minimise potential trauma. Granting leave in such situations is a common practice in newsrooms.

Depending on the severity of the threat, the journalist could also be relocated or reassigned to protect his or her life.

### Public statement of support

For the news organisation, showing public support for a journalist under attack sends a clear message that the organisation stands behind its staff and views attacks on its journalists as an attack on the institution as a whole.

However, these factors should be considered before a statement is issued:

- Will it amplify the attack?
- Will it lead to further harassment?
- Will it harm any legal case that the news organisation is considering filing?

## Moderating online content

A thorough, and well-developed strategy for moderating user comments is necessary. You may already have a system in place to remove spam comments or hate speech, and it should be extended to include unacceptable attacks on journalists and news organisations. (Note: this should not extend to legitimate criticism.)

Take the following preventative steps against online abuse:

- Develop and prominently share community guidelines that can serve as key tools for both users and moderators. These participation guidelines will make clear that criticism is welcome, but insults, attacks, hate, and threats will not be tolerated. Refer to the [Guardian's community standards](#) as a guide.<sup>22</sup>
- Set up a registration scheme on your website. It is good practice to ask users to register to be able to comment. This requirement is important not only in view of potential legal liabilities but also as an initial hurdle to dissuade aggressors and machine-operated accounts.
- Block the ability to comment at certain times. If there are times, such as overnight or during weekends, when moderators cannot dedicate sufficient time to the task, consider blocking the ability to comment for the relevant period of time. If you do so, make sure to inform your users when they will be able to post comments again.

When moderating and reacting to online abuse, keep in mind that removing online attacks, threats, and insults targeting journalists does not eliminate the risk of physical violence emanating from the aggressor.

Moderators who see aggressive messages aimed at a journalist, particularly those that contain a threat, should not only remove those messages, but record them first,

---

<sup>22</sup> The Guardian. 2022. The Guardian website community standards and participation guidelines. [online] Available at: <<https://www.theguardian.com/community-standards>> [Accessed 14 February 2022].

and bring them to the attention of relevant persons in the news organisation, including the target of such attacks.

When dealing with comments left on your own site:

- Removing comments: Comments that do not fall within the confines of legitimate criticism and are in breach of the community guidelines, even if they do not threaten a journalist, should be recorded, reported, and removed. It is good practice to inform users why their comments were removed.
- Warn users who repeatedly breach the community guidelines. A good way of doing so is to block their ability to post comments for a period of time.

When dealing with comments left on social media, remember: record, report, remove. Familiarise yourself with tools available on specific platforms, and adopt platform-specific strategies. For example:

### Facebook

- Delete a comment when it contains aggressive or threatening content or derogatory words and insults.
- Ban a user from the media outlet's Facebook page when the user has repeatedly posted hateful or abusive comments, even after being warned.
- Remove a user from the page as a warning to deter further abusive comments.
- Disable/turn off comments. Consider doing this when there are very limited resources available to moderate content.

### Twitter

- Block words and set the strength of the profanity filter.
- Report a post, page, or user that has breached social media's own community standards.

- [Muting](#): Consider muting a user when their posts are in violation of your community standards. Muting a user removes their activities from your timeline. This tool is available on Twitter.<sup>23</sup>
- **Blocking**: Moderators generally adopt this measure as a last resort, tending to block accounts that persistently spam or send scams. Note that since the moderator will not be able to access the blocked account, it makes it difficult to monitor any imminent threat.

## Security Training

Provide basic online security training to all journalists and freelancers in your newsroom.

- Train journalists to identify and use end-to-end encryption apps for communication (e.g. [Signal](#)).<sup>24</sup>
- Encourage journalists to use a secure email service (e.g. [Proton Mail](#)).<sup>25</sup>
- Ensure journalists use strong passwords. Refer to Google’s [guidelines](#) on how to create a strong password.<sup>26</sup>
- Train journalists to use two-factor authentication for log-in approval.
- Encourage journalists to check a site’s URL for secure protocols. Does the URL start with “http://” or “https://”? An s at the end means the connection is encrypted and secure, so any data entered will be safely sent to the website. Avoid sharing any personal information on websites without this added layer of security.

---

<sup>23</sup> Blog.twitter.com. 2022. Another way to edit your Twitter experience: with mute. [online] Available at: <[https://blog.twitter.com/en\\_us/a/2014/another-way-to-edit-your-twitter-experience-with-mute](https://blog.twitter.com/en_us/a/2014/another-way-to-edit-your-twitter-experience-with-mute)> [Accessed 14 February 2022].

<sup>24</sup> Signal.org. 2022. [online] Available at: <<https://signal.org/en/>> [Accessed 15 February 2022].

<sup>25</sup> ProtonMail. 2022. Secure email: ProtonMail is free encrypted email.. [online] Available at: <<https://protonmail.com/>> [Accessed 15 February 2022].

<sup>26</sup> Support.google.com. 2022. Create a strong password & a more secure account - Google Account Help. [online] Available at: <<https://support.google.com/accounts/answer/32040?hl=en>> [Accessed 15 February 2022].

## Additional tools and resources

- Money Trail and Free Press Unlimited have a free resource on security training for newsrooms and journalists, which can be accessed [here](#).<sup>27</sup>
- [The Media Legal Defence Initiative](#) provides legal help to journalists, citizen journalists, and independent media worldwide.<sup>28</sup>
- [The International Women’s Media Foundation](#) offers safety training, reporting trips, and byline opportunities – all tailored to women journalists, both established and up-and-coming.<sup>29</sup>
- The [Committee to Protect Journalists](#) defends the right of journalists to report the news safely and without fear of reprisal.<sup>30</sup>
- The [Global Investigative Journalism Network](#) provides free monthly training programmes for journalists across Africa.<sup>31</sup>
- The [International Federation of Journalists](#) has a “safety fund” that offers financial assistance in a range of emergency cases such as threats, violence, prosecution, settlement in exile, and illness.<sup>32</sup>
- [Pen International](#) supports journalists at a grassroots level to protect, shelter, and resettle writers at risk globally.<sup>33</sup>
- [Article 19](#) does advocacy on digital rights and media freedom.<sup>34</sup>

---

<sup>27</sup> Security\_HQ. 2022. Training Material. [online] Available at: <<https://security.money-trail.org/training-material>> [Accessed 16 February 2022].

<sup>28</sup> Mediadefence.org. 2022. Homepage - Media Defence. [online] Available at: <<https://www.mediadefence.org/>> [Accessed 16 February 2022].

<sup>29</sup> Iwmf.org. 2022. Home - IWMF. [online] Available at: <<https://www.iwmf.org/>> [Accessed 16 February 2022].

<sup>30</sup> Committee to Protect Journalists. 2022. Committee to Protect Journalists – Defending Journalists Worldwide.. [online] Available at: <<https://cpj.org/>> [Accessed 16 February 2022].

<sup>31</sup> Malik, A., Hasan, M. and Chitra, R., 2022. Global Investigative Journalism Network. [online] Global Investigative Journalism Network. Available at: <<https://gijn.org/>> [Accessed 16 February 2022].

<sup>32</sup> IFJ. 2022. Safety Fund - IFJ. [online] Available at: <<https://www.ifj.org/safety-fund.html>> [Accessed 16 February 2022].

<sup>33</sup> PEN International. 2022. PEN International – Promoting literature and freedom of expression. [online] Available at: <<https://pen-international.org/>> [Accessed 16 February 2022].

<sup>34</sup> ARTICLE 19. 2022. ARTICLE 19 - Defending freedom of expression and information.. [online] Available at: <<https://www.article19.org/>> [Accessed 16 February 2022].

- [Shelter City](#) provides human rights defenders including journalists who are threatened because of their work a shelter in the Netherlands.<sup>35</sup>
- [Dart Center](#) has a resource unit which provides mental health support for journalists who suffer trauma as part of their work.<sup>36</sup>

---

<sup>35</sup> Sheltercity. 2022. About us - Sheltercity. [online] Available at: <<https://sheltercity.org/about-us/>> [Accessed 16 February 2022].

<sup>36</sup> 2022. [online] Available at: <<https://dartcenter.org/resources?keyword=psychological>> [Accessed 16 February 2022].

## Assign roles and tasks

Addressing online abuse effectively requires the adoption of new roles and tasks in the newsroom, both for editors and journalists, and for managers and moderators.

Primary among these is the Online Safety Coordinator role. This can be assigned to a single individual as a full-time role or, if there are resource constraints in the media organisation, can be shared by multiple staff members who report to a task force leader. These are the key tasks that need to be adopted.

### Online safety coordinator

- Acts as a figure to whom journalists can report incidents of online harassment.
- Assesses, in coordination with the targeted journalist and their editor, each case of online harassment and suggests support mechanisms for the targeted journalist.
- Where necessary, coordinates with management and legal experts on any institutional response by the media outlet.
- Keeps a database of online abuse cases updated, allowing the team to evaluate the efficacy of measures implemented.
- Due to the changing nature of online attacks, regularly review the measures that the newsroom has in place to prevent and respond to online harassment.
- Acts as a coordination and educational point for these measures. The online safety coordinator should be deeply familiar with all newsroom measures, able to explain them to journalists facing online abuse, and the primary point person for their implementation.
- Regularly attends editorial meetings to become aware of upcoming content that may trigger online abuse.

## Management

- Acknowledges that online harassment is a serious concern and that an attack on one staff member is an attack on the entire media organisation. Regularly communicates this position to the newsroom.
- Adopts structural changes in the newsroom – including the appointment of one or more Online Safety Coordinators (as described above) – to create an environment in which reporting online abuse is not stigmatised. Ensures that sufficient resources, time, and funding are allocated to maintain and update these new structures.
- Includes the targets of online attacks in decision-making processes that affect them.

## Editors

- Acknowledge that online abuse is a serious and unacceptable issue and not simply a characteristic of modern journalism, or a rite of passage.
- Regularly include online harassment as a topic in editorial meetings. Speaking openly about the issue will create an atmosphere in which journalists will feel more comfortable reporting attacks.

## Moderators

Note: Moderators may include those employed to oversee comment sections or other submissions on owned-and-operated platforms, as well as social media editors and audience team members moderating content on external platforms.

- Identify individual threats and orchestrated campaigns on social media platforms and comments sections targeting staff members, record them in a database, and escalate them to the journalist, editor, and online safety coordinator.
- Help assess the threat level of the online abuse.

- Assist in managing targeted journalist's social media accounts to reduce their exposure to violent content and minimise potential trauma.

## Journalists

- Understand that online abuse is a serious and unacceptable issue and not simply a characteristic of today's journalism.
- Participate in all relevant training opportunities offered by the media outlet, including awareness, digital security, and trauma risk management training.
- Participate in both formal and informal peer support structures.
- Report issues of online abuse when they occur, even if the journalists do not believe they will suffer any negative consequences from the abuse. Reporting these incidents helps the newsroom understand the scope of the issue and develop the measures necessary to counter it.

# Acknowledgements

First, I would like to thank the Reuters Institute at Oxford University for the institutional support I received in producing this guideline, particularly from Caithlin Mercer, Meera Selva, Rasmus Nilsen and Philippa Garson.

I also appreciate the peer support I received from my colleagues and research fellows at the Institute, and thank my family for their continued support throughout my career.

Appreciation is also due to my colleagues at iWatch Africa, and staff at the Center for International Media Assistance – particularly Daniel O'Maley, whose years of background work significantly shaped this output.

Particular thanks also to news editors and journalists such as Marian Ansah, Elfredah Kevin-Alerechi, Paul Kamtchang and Mohammed Kabba who offered their insights into the conversation about journalists' safety online.

Thank you all for the support.