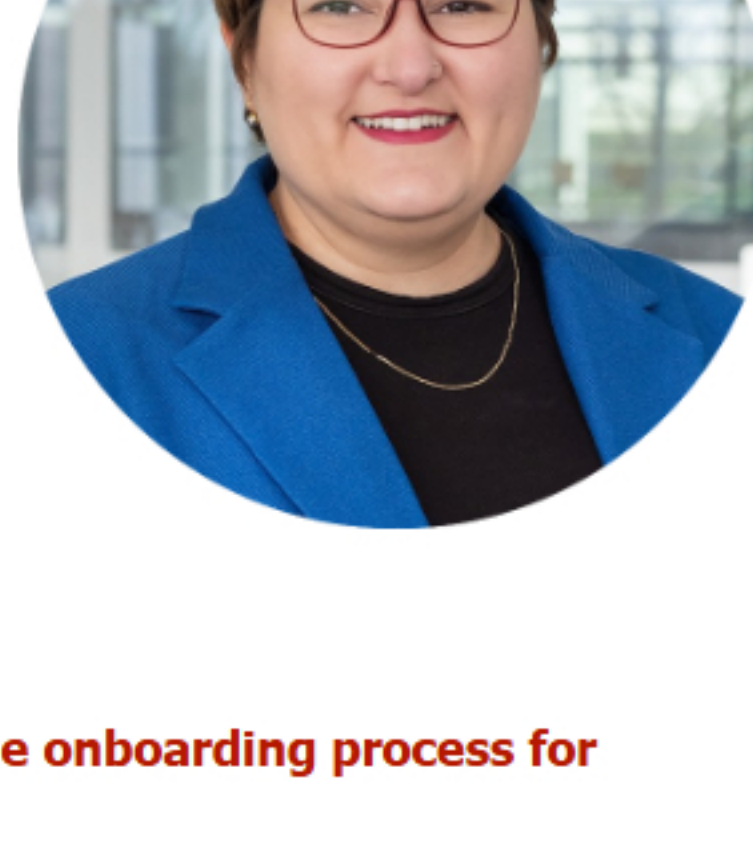


As we prepare for the new year, we are adapting our strategies and making plans. We may also propose expanding the team or launching new forms of interaction with the community. **But how can we organize the process of integrating a new person into the team while being vigilant** and caring for internal and external security and the team's well-being? We discussed this issue with Yasmina Al-Gannabi, the social media security officer at Deutsche Welle.

Yasmina Al-Gannabi
Social Media Security Officer at Deutsche Welle



From a security perspective, what does the onboarding process for journalists look like?

In this case, we are talking about two important levels. The first level is about access to corporate accounts for people who will need to manage online communities or produce content, and the second level is about keeping their private accounts secure.

Typically, we encourage departments to grant access only through the management system on platforms like Meta Business Suite or YouTube Creator. Individuals who are live streaming or want to use the collaboration feature on Instagram may only log in directly to the app in individual cases. Only two or three people, including content coordinators and department leaders, receive administrator rights. These individuals can monitor work pace and vacation schedules. To avoid situations where people connect from public networks or hotels, we temporarily revoke access for those who go on vacation.

A lot of maintenance work follows the initiation process. For example, we check every two months that access is in order and that no foreign applications are connected that could pose a risk. You may see an advertisement on Instagram, download an app, log in, and then forget about it. However, access to it remains. For this reason, we check and remove any tools that have not been approved at the organizational level. We only use tools that have been verified by our IT team. This demonstrates our commitment to responsibility, particularly towards our users in countries with sensitive security contexts.

At what point is it appropriate to give new colleagues access to our work platforms?

In order to give people access, you need to trust them. For my team, this takes at least two or three months because, as a new employee, you may feel overwhelmed by the amount of information you receive. In this context, mistakes are possible. That's why I need to ensure my colleagues fully understand all the processes first.

Editors should be ready to work from day one when hired, but I encourage teams to wait at least a month before granting new hires access to the platforms.

What criteria can we use to define trust when providing access?

It's important for new team members to understand our role and the types of tasks we perform. One of the first tasks I usually assign to new colleagues is to conduct research and assist me with presentations. Once I see that they are doing well, I give them a final training session in which I clearly explain that access comes with a great deal of responsibility.

As members of the Audience Development team, we have access to all Deutsche Welle accounts. If something were to happen to one of us, it could affect the entire organization's system. Having access to the password management system poses a significant risk. That's why I make sure they understand that they can only use work devices and that they cannot use public Wi-Fi while working. I also explain how they should protect their devices while traveling. We also have a checklist that team members need to review periodically to ensure that everything is in order. Fortunately, no one has encountered any issues so far. Although it may seem like a lot of work at first, it is worth it in the long run.

Which risks are you trying to prevent?

Even when your account hasn't been hacked, I think one of the biggest risks is doxing. (Doxing is the deliberate publication of a person's personal information without their consent with the aim of intimidating them – editor's note). People greatly underestimate the danger of doxing. Unfortunately, there have been enough cases like this. This can happen not only to you, but also to someone close to you, such as a family member or friend. Even if you keep your personal and work accounts separate and use different names for each, there is still a risk of exposure. It only takes one person close to you to have their account hacked and use it to access your private information. We know we need two-step authentication and that we have to work on work devices and use systems like Meta Business Suite, but we suddenly become much more careless when it comes to our personal lives and private data.

There was an incident with a colleague who was broadcasting live on our corporate Facebook account. It was a casual conversation, and at one point, she mentioned that she lived in the neighborhood, just a two-minute walk from the café where the broadcast was taking place. I saw two users writing to each other in the comments: "I told you I saw this anchor in the neighborhood, but you didn't believe me. Look, I recognize the café. Why don't we go there tonight? Maybe we'll run into her." We obviously had to stop the live broadcast because it had become risky.

A few years ago, my mother's account was hacked. She didn't realize it had happened because the hacker didn't immediately start posting on her behalf. However, by accessing her account, the hacker was able to gather information about me and my family and open a new account, posting certain details. Fortunately, it wasn't extremely sensitive information, but it was enough for me to realize that I needed to educate my mother about online safety to protect us both.

Even if these things don't physically harm you directly, they scare you. At some point, you won't know how this information could be used against you.

In what ways can journalists maintain a public online presence while remaining vigilant?

There are several types of rules within the institution. We at Audience Development developed guidelines for using social media in collaboration with various internal departments, such as the legal and editorial teams. Then there are the impartiality rules established by the editor-in-chief and the editorial board. As a public radio and television station, we have responsibilities regarding our opinions and beliefs.

Within the organization, we oversee the Newsflencer and Ambassadors projects. The Ambassadors project involves colleagues selected by the Corporate Communications Department to act as brand ambassadors. They showcase what goes on behind the scenes at Deutsche Welle, our values, what it's like to work for us, and the opportunities available. They are mainly active on LinkedIn and, to a lesser extent, Instagram. They have set their own rules about how much they can share about their private lives.

Newsflencers are people selected from different departments. We are still developing this concept, which obviously means establishing specific contracts with them. They already have their usual contract with Deutsche Welle. In addition to this, there is a supplementary contract that clarifies several things, such as how far we can go as an institution in analyzing content and how much we can get involved in community management and checking private messages and data. This is already a separate area of work.

We also set limits on product placement. Colleagues often ask us if they can promote a particular product. We have to consider whether the product aligns with Deutsche Welle's values. For example, we don't encourage our newsflencers to promote alcohol on their accounts. However, if the promotion were of sustainable fashion in Guatemala and our colleague knew someone there who wanted support, that wouldn't be a problem.

What about the other staff members? What rules do they have to follow?

It's mainly about impartiality and human rights-related content. If someone posts something that goes against these values, then it's a problem. This does not mean that we check employees' private social media accounts. We don't have the resources to do so, nor do we want to. However, if a department head sees a problematic social media post, they can first have a private discussion with the employee and then involve our mediation team.

At Deutsche Welle, we have a mediation team that intervenes and provides support in such situations. These teams are relatively new, having been established during the pandemic when we realized how important they are.

These rules are constantly updated. Each person must read them and confirm in their internal profile that they agree to them. This applies to everyone, including freelancers, interns, and partners.

How can we manage how reporters interact with the public?

One of our goals this year was to increase interaction between reporters and the public. It is important to us to implement this goal as often as possible.

Colleagues who moderate comments and interact with the audience always use official accounts for corporate accounts, unless they are part of the Ambassador Team or the Newsflencer Project.

You won't see regular editors commenting from their personal accounts. This is not encouraged. Unfortunately, many years ago, a colleague was attacked with racist comments. She was so affected by this that she got into an argument with the commenters from her personal account. Thus, people who didn't know she was on Instagram or Facebook found her there, and she essentially doxed herself. At the end of the day, we are all human. It only takes one comment to trigger you, causing you to give in and engage in direct conflict with users. I strongly believe in the idea of "not feeding the trolls."

What role does mental health play in discussions about vigilance?

There are several levels here. The first concerns the people who manage the community. Our colleagues are confronted with hate messages every day, and it's easy to lose faith in humanity. Speaking from my own experience, when I started working at Deutsche Welle, I was a community manager for the Kuwaiti audience. It was an extremely difficult period, and we were confronted with complicated images daily. I also did fact-checking. Our job wasn't just to moderate comments, but also to check content sent by users. People sent us images and videos, and we had to determine whether we could use the content. Imagine seeing images of blood and violence every day. I think the same is true for my colleagues who are now working on the Ukraine story. At some point, it starts to affect your personal life.

Statistics show that women are the primary victims of this type of harassment. The problem is that we are so accustomed to it that we only take harassment seriously when it becomes an explicit threat to us or our families.

Another aspect related to mental health is the constant pressure to be "up to date" with the latest trends and demands in the media industry. Working in a newsroom requires you to fulfill several roles, such as video creator, show host, editor, and online community moderator. These roles can increase stress levels.

Many people have developed their own emotional regulation mechanisms during the pandemic, but this is still not enough, especially when new challenges arise, as with our colleagues in Ukraine. I remember holding a workshop for the Ukrainian department just a few weeks after the Russian invasion. I don't remember exactly what I said, but it triggered a reaction in one of my colleagues who started crying. We had to abandon our initial plan for responding to hate speech and worked together to find emotional regulation mechanisms for someone directly affected by the war who still has family in Ukraine. Situations like this, where emotions like uncertainty, fear, and helplessness build up, make it clear that mental health can't be ignored.

In what ways does artificial intelligence influence these changes?

One of the major challenges is the creation of deepfakes. The faces of TV presenters and show creators are used in problematic videos. I'm not just talking about sexual content; I'm also talking about clips in which these people appear to commit crimes or engage in compromising activities.

As individual organizations, I believe that we cannot do much on our own. However, if we join forces with other organizations and advocate for these issues, we hope to raise awareness among the population and politicians. Politicians can then create a clearer legal framework regarding the use of AI, fake news, and deepfakes.

What skills do you need to develop as a young journalist?

I believe that, without underestimating their skills and knowledge, the issue of sources remains very present for young journalists. We work with many students who attend training sessions or apply for internships in our teams. I was surprised by their insufficient level of responsible news consumption. For example, they don't pay attention to the source. When they see a video on TikTok, they say, "Okay, I saw it on TikTok," but they don't check the account that posted it or verify the credibility of the information.

What is some practical, easy-to-implement advice for small organizations?

Choose your battles wisely. Don't try to be everywhere; focus only on areas where you can provide the most value to yourself and your audience. If you find that engaging with the community and being present in comments adds more value to the conversation and increases the visibility of the topics you believe in, even if it means producing less content, then that's fine. When it comes to tools, don't focus too much on them. It's best to start with what's currently free and accessible. When you have the financial resources, you can invest in more sophisticated tools.



Opportunity!

Reporters Without Borders (RSF) have launched the platform **RSF Resources for Journalists**. The platform offers practical and user-friendly resources to help journalists protect themselves, educate themselves, and work safely, even in hostile environments. It hosts over 150 articles and materials organized by topics such as digital safety, physical safety, mental health, and legal advice.



Get Help!

If you are experiencing ongoing stress and anxiety, you can request a free and confidential consultation with a psychologist using **this chatbot** or by filling out **this form**. You will be connected with a specialist within 48 hours.

If you liked what you read, please recommend our newsletter to a colleague. Feedback helps us get better. Let us know what you think about the newsletter at api@api.md.