Does Your Workplace Harassment Policy Need a Digital Makeover?

You can't fight digital harassment with an analog policy.

You might think that employees are less vulnerable to workplace harassment when they work from home. But you'd be wrong. Since the pandemic began:

- More than 4 in 10 U.S. workers (41%) reported that they've been subjected to some form of digital harassment (Pew Research);
- Nearly half (45%) of women experiencing sexual harassment say it happened remotely (Rights of Women, UK and Wales ("ROW"));
- 23% of women reporting that they've been harassed say the problem has increased since they began working from home (ROW); and
- More than 7 in 10 (73%) of victims say they don't think their employer is doing enough to protect them from remote harassment (ROW).

Far from eliminating workplace harassment, the migration of employees to the home office has only caused it to go virtual. Cyberbullying, hate speech, stalking and other similarly nasty behaviours have thrived in pandemic conditions. Purveyors of harassment have also gotten better at using video conferencing, social media platforms, virtual discussion groups and other technologies to unleash new forms of harassment like zoom bombing, doxing and dogpiling.

The symbolic "coming out party" of digital harassment occurred last November when highly renowned magazine writer Jeffrey Toobin exposed his genitals to co-workers during a Zoom call. Toobin quickly apologized and claimed he didn't realize he was actually on camera. But the damage was done. After Toobin's suspension, Twitter users went online to share their own workplace harassment war stories under the #MeToobin hashtag.

Unfortunately, employers haven't adapted nearly as well. As employer, you're legally obligated under OHS, human rights and other laws to protect your employees from workplace harassment regardless of where they happen to work. But you can't prevent digital harassment with old-fashioned policies designed for analog threats. What's needed, and rather urgently, is for employers to review and, if necessary, revise their harassment policies to deal with the new face of harassment. Specifically, there are 5 ways you may need to broaden your current harassment policy to protect employees from digital threats.

1. Broaden Definition of “Harassment”

Pitfall: Standard policy definitions of “harassment” list forms and examples of prohibited conduct—name-calling, threats, stalking, etc. But the focus is typically on in-person behaviour with no mention of online harassment. This critical policy omission may add to the false sense of security some employees experience when they’re behind a computer screen and embolden them to make comments that they wouldn’t dare utter to a co-worker in-person.

Solution: Make sure your policy definition covers common forms of online harassment that employees are likely to commit or experience, including:

- **Hate speech**, which you should define narrowly as including communication that attacks, discriminates or uses pejorative language to induce hatred, contempt or violence against a person or group on the basis of their race, colour, descent, sex, religion, ethnicity, etc.;
- **Cyberbullying**, or willful and repeated harm inflicted via computers, cell phones and other electronic devices;
- **Impersonation**, or posting harassing comments, photos or other materials in somebody else’s name, typically in an attempt to get that person into trouble;
- **Swatting**, a dangerous (but thankfully, relatively rare) form of impersonation involving online threats designed to get a SWAT team to bust down the impersonated individual’s door;
- **Hacking**, whether it’s done to steal personal information, sabotage an IT network or simply harass somebody;
- **Denial-of-Service (DoS) attacks**, i.e., flooding a host or network until it crashes in a malicious attempt to prevent employees, customers and other legitimate users from accessing an organization’s website;
- **Doxxing**, or collecting documents (docs) containing an individual’s private information and posting them online for all the world to see and use;
- **Trolling**, or posting nasty and provocative things online in an attempt to upset, instigate and stir up trouble;
- **Dogpiling**, which is a form of trolling typically carried out by hundreds and even thousands of people seeking to overwhelm a website or social media page by posting negative comments on it at the same time; and
- **Message bombing**, which is similar to dogpiling that targets inboxes to make it impossible to respond to legitimate messages.

2. Broaden Definition of “Workplace”

Pitfall: One of the hallmarks of an obsolete harassment policy is its limitation to the organization’s facility or at organization-sanctioned events. This is out of step with not only digital threats but also the OHS law duty to prevent harassment in the “workplace,” which is broadly defined to include any site where employees carry out their employment duties on the employer’s behalf.

Solution: Make sure your policy definition of “workplace” covers all forms of carrying on business and all work-related settings where harassment can occur (including after-hours), including:

- Home work spaces;
- Client and customer visits and service calls;
- Business travel;
- Conferences, training sessions and seminars;
- Organization- or client-sponsored social functions;
- Other offsite work assignments.

Model Language: *For purposes of this policy's ban on workplace harassment, "workplace" means anywhere where ABC Company employees are conducting business on the Company's behalf, including but not limited to, conducting business in person on Company premises or from a home or remote setting, on the phone, virtually, or through email or other social media and/or during after-hours events such as, but not limited to, business meetings, dinners, trainings, and during work-related travel.*

3. Implement Code of Conduct for Remote Meetings

Pitfall: The virtual meeting has become the digital age version of the holiday office party where employees feel like the normal rules against acting like a pig don't apply. Regrettably, old school harassment policies are ill-suited to these venues.

Solution: Whether as part of your current harassment policy or in a separate policy, create and strictly implement a written code of conduct for remote meetings. Like the template on the HRI website, make sure your code:

- Clearly states that your workplace harassment policy applies to remote work and virtual meetings;
- Specifically defines what conduct is unacceptable;
- Addresses the reporting and investigation of complaints; and
- Provides for discipline against those who commit violations.

4. Guard Against Digital Harassment from Third Parties

Pitfall: In a recent study, researchers reviewed the workplace harassment policies of 129 universities and colleges across Canada and found that only 41 one of them acknowledged online harassment. They then analyzed those policies and found a common flaw: the policies were designed to protect employees and students against harassment committed by other people **at the** institution. The problem is that the employees and students who actually experienced online harassment reported that it usually came from people outside of or unknown to the institution.

Solution: Your commitment to protect employees from workplace harassment should cover harassment from all sources, not just other people at the organization, including customers, clients, contractors and their employees and unknown third parties.

5. Ensure Employees Can Report Harassment Remotely

Pitfall: Another potential disconnect to check for is whether your policy requires employees to be present on the site to report the harassment they experience.

Solution: Make sure there's an online mechanism for telecommuters and other remote employees to report harassment to HR. Emphasize that you'll take all harassment complaints seriously and investigate them promptly, regardless of whether they're submitted in-person or online.