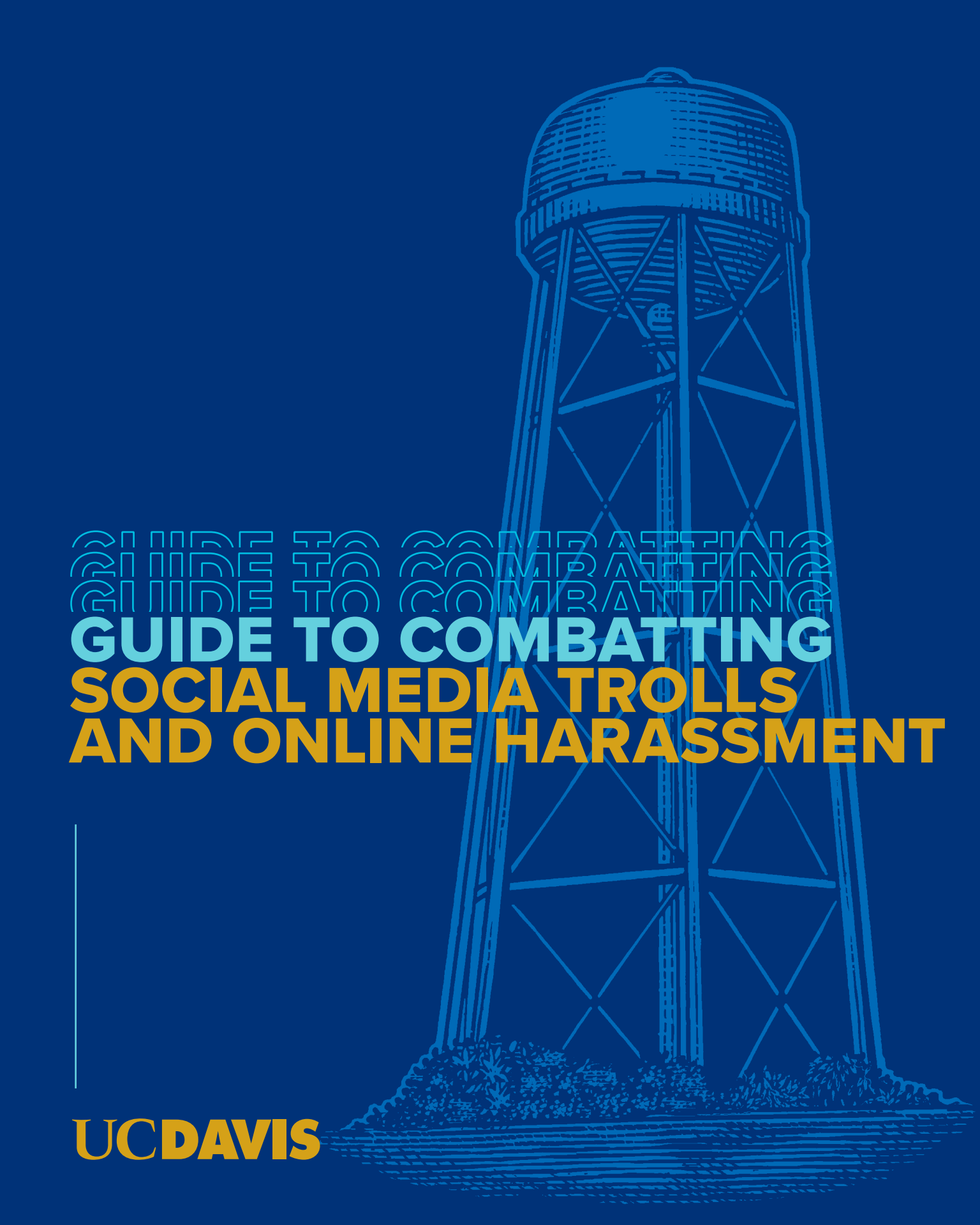

GUIDE TO COMBATTING SOCIAL MEDIA TROLLS AND ONLINE HARASSMENT

UC DAVIS

Online harassment can occur when digital technologies (social media, email, text message, gaming platforms or other messaging services) are used to post unwanted, inaccurate, or threatening content specifically targeting an individual or group.

Behaviors that could potentially be considered online harassment include remarks that a reasonable person would perceive as seriously alarming, seriously annoying, seriously tormenting or seriously terrorizing of the person and that serves no legitimate purpose which can include impersonation, threats, revealing personal information, cyber stalking, or sending unsolicitated sexual messages or images.

PART ONE

Actions to Take if You Are the Target of Online Harassment

Actions to take if you are a target of online harassment

Step One. Assess the Threat.

Call the police. If you or your family (or another identifiable group) appear to be in imminent danger, call 911 immediately! If you receive threats that you feel are serious but not imminent, call the UC Davis Police (Davis non-emergency line 530-752-1727 / Sacramento Campus non-emergency line 916-734-2555).

Step Two. Gather Evidence.

Document it. Take screenshots of potentially harassing messages or posts and save the unique links to posts or messages in a separate document. Be sure to grab information about the user or handle names, their real name, the links to their profiles and any other information about the source of the harassment. This information will be useful to your department chair, IET, case workers or police units who may be assisting you and could be used as evidence.

Step Three. Get Support.

For faculty. Connect with your administrative leader (department chair, the dean's office, lab lead, other) and the communications teams from your college.
For staff and student employees. Reach out and alert your supervisor right away, especially if the harassment may be in relation to your work.

CALL 9-1-1 IF YOU FEEL YOU OR YOUR FAMILY ARE IN IMMINENT DANGER.

Step Three. Get Support. (Continued)

Ask for help before responding to media.

If you get contacted by the media, you are not obligated to return the call. Reach out immediately to the News and Media Relations team at Strategic Communications who will help you sort through the next steps at 530-752-1930 or **news@ucdavis.edu**.

Ask for your personal information to be temporarily removed from the campus directory and webpages and social media. You can ask for your contact information to be removed from the campus directory, department webpages or even have posts removed from campus social media accounts if necessary. Staff and faculty should work with campus IET for help with directory listings. Students can request a confidential registry listing through the Office of the Registrar. Additionally, if you have other web pages (such as Square Space, WordPress, etc) turn off commenting features and remove any features that allow commenting, emailing or contact. These features can always be turned back on after the online attack passes.

Step Four. Secure Your Social Media Boundaries.

Revisit your privacy settings. Social media platforms all have privacy settings that can help mitigate the impact of strangers who can contact you or post comments. These settings give you the power to choose who can see your profile, who can message you, who can tag you and how much information is shared from social media publicly. Each platform is different and privacy settings change frequently. For links to social media platform privacy settings pages, visit **communicationsguide.ucdavis.edu/departments/social-media/policy-and-guidelines/trolling-guide**.

Change your passwords. As an extra precaution, change your passwords to new and secure passwords to preempt any hacks. Enable two-factor authentication where possible.

Take a social media break. Trolling attacks are typically intense but brief. Engaging with these comments tends to add fire to the flame and it's best to not engage. It can help to take a social media break by temporarily removing social media account apps from your phone, which can alleviate distressing notifications or the urge to check social media.

Mute and Block. All social media platforms have the ability to mute or block users from accessing your social media content. On Facebook, Twitter and Instagram you can choose to "mute" an individual or a post. Muting is a great option if you don't want to completely remove that person from accessing your social channels but want to silence notifications and conversations from them. Muting does not unfriend or block a user.

TIPS

Additional support resources.

You don't have to go through this alone and we have support resources to help you navigate several different situations.

UC Davis Police

Davis Campus Police

EMERGENCY: 911 or 530-752-1230

Non-Emergency: 530-752-1727

Sacramento Campus Police

EMERGENCY: 911 or 916-734-2555

Non-Emergency: 916-734-2555

Online: Report a hate or bias incident

hdapp.ucdavis.edu

Office of Student Support and Judicial Affairs (OSSJA)

530-752-1128

ossja@ucdavis.edu

Academic and Staff Assistance Program (ASAP)

UC Davis employees - call (530) 752-2727

UC Davis Health Employees - call (916) 734-2727

Student Health and Counseling Services

Students can schedule mental health appointments online through Health-e-Messaging, or by calling 530-752-0871.

Step Four. Secure Your Social Media Boundaries. (Continued)

You also have the ability to block users that you don't want accessing your content or leaving comments. You do not owe anyone an explanation about why you've blocked or unfriended them. (Note: University-run accounts need to go through a different and official process and involves different considerations before blocking or muting can occur).

Report it to the platform. Each social media platform has a process for reporting users who are engaging in harassing behaviors, making threats or impersonating you. Most platforms act quickly on these reports, especially if they receive more than one report. Once verified that the offending actions are against platform harassment policies, the platform will take action to delete the user comments and accounts per their policies. In extreme cases, users can be banned outright from using the platforms. Activate your support network and ask them to also file a report on the content or profile in question. These reports are also used for any police case filings or warrants.

When the storm has passed, do a Google audit. Once the attack has passed, do a google search on your name to understand what records google has picked up around your name or the issue at hand. This is helpful information to know and there are some actions you can take, such as claiming your Google profile (if eligible) that can help stabilize search results. It is not recommended to do this in the heat of the attack - it can be very overwhelming.

communicationsguide.ucdavis.edu/departments/social-media/policy-and-guidelines/trolling-guide

PART TWO

Checklist for Academic Leaders and Supervisors Supporting Employees or Students Experiencing Online Harassment

Checklist for Academic Leaders and Supervisors Supporting Employees or Students Experiencing Online Harassment

Online harassment is the repeated use of digital technologies (social media, email, text message, gaming platforms or other messaging services) to post unwanted, inaccurate, or threatening content specifically targeting an individual or group. These attacks generally single out an individual and can be professionally disruptive and upsetting.

Supervisors and academic leads are often the first point of contact to start the process of assisting scholars who find themselves targeted by online harassment.

These incidents can be very intense and frightening and often escalate quickly. Moving quickly is important to support the scholar or students who are impacted.

Step One. Evaluate if Immediate Action Is Needed.

Call 9-1-1 if the employee, their family, or an identifiable group (for example, a class) are in imminent danger.

See resources and contacts below for situations that are serious, but harm is not imminent.

Step Two. Document It.

Working together with the employee affected, take screenshots and save the unique links to posts or messages in a separate document. Be sure to grab information about the user or handle names, their real name, the links to their profiles and any other information about the source of the harassment.

CALL 9-1-1 IF YOU FEEL YOU OR YOUR FAMILY ARE IN IMMINENT DANGER.

Step Two. Document It. (Continued)

This information will be useful to get other support units up to speed quickly and uniformly on the situation and can be used as evidence. Please note that some documentation, such as emails and text messages, can be privy to public information requests. Keep that in mind when creating any documents.

Step Three. Confirm that the UC Davis Police Department and responses teams have been contacted, if needed.

If not, do so immediately. Provide whatever documentation you have collected so far to the police department and to the appropriate response teams.

Step Four. Provide Resources.

Share with the employee the link to “Actions to Take if You Are a Target of Online Harassment” guidance and share Academic and Staff Assistance Program (ASAP) information for support.

Step Five. Mobilize the Following Response Teams and University Resources.

IMMEDIATE RESPONSE TEAM

UC DAVIS POLICE DEPARTMENT

Davis Campus: 911 or 530-752-1230

Sacramento Campus: 911 or

916-734-2555

WORKPLACE VIOLENCE COMMITTEE (FOR EMPLOYEES)

Resources and contact information to report for non-emergency workplace intimidation, threats or acts of violence.

STUDENT CONCERN RESPONSE TEAM (OSSJA)

OSSJA coordinates the Students of Concern Response Team (SCRT), an interdisciplinary group of professionals that manages situations involving students of concern who present with serious risk of harm to self or others. This team of UC Davis staff and law enforcement professionals meet on a weekly basis and when needed to ensure a comprehensive approach to students of concern.

UNIVERSITY RESOURCES

DEAN'S OFFICE

Inform the dean's office as quickly as possible. The unit administration can assist with everything from identifying alternate space for classes to ensuring that campus administration services are mobilized.

PROVOST'S OFFICE

Together with the dean's office, contact the Office of the Provost. Provide the documentation and the provost's office can activate leadership.

HARASSMENT AND DISCRIMINATION ASSISTANCE AND PREVENTION PROGRAM (HDAPP)

530-747-3864 (Davis Campus)

916-734-3417 (Sacramento)

HDAPP assists individuals and campus units to resolve conflicts and complaints related to harassment, discrimination, sexual harassment, sexual violence and hate and bias and serves as the central office for receiving reports and maintaining records of these types of complaints. Email: **hdapp@ucdavis.edu**.

ACADEMIC AFFAIRS

Academic Affairs can help academic leaders with conflict management, and engaging in problem-solving to help reduce potential liability.

INFORMATION TECHNOLOGY SERVICES (IET)

(530) 754-4357 | **cybersecurity@ucdavis.edu**

Alert IET (or the department's IT) to help begin managing the scholar's email, directory listing, and online presence.

Step Five. Mobilize the Following Response Teams and University Resources. (Continued)

UNIVERSITY RESOURCES (CONTINUED)

STRATEGIC COMMUNICATIONS

530-752-1930 | **news@ucdavis.edu**

Strategic Communications will handle any incoming media inquiries, social media impacts and support, and will coordinate with the college's communications professionals to assist with a communications strategy and any statement that may need to be written.

ACADEMIC AND STAFF ASSISTANCE PROGRAM (ASAP)

UC Davis (530) 752-272

UC Davis Health (916) 734-2727

ASAP offers confidential, cost free consultation and referral services to all UC Davis and UC Davis Health faculty, staff and their immediate families.

OFFICE OF CAMPUS COUNSEL

Campus Counsel works together with Strategic Communications should any communications need to be issued or if legal action is potentially necessary. Note: Campus Counsel does not provide legal advice to individual faculty, staff, or students.

Step 6. Prepare Teams for Potential Impacts.

Prepare staff to handle phone calls, emails, social media comments and inquiries about the harassment issue. If an approved statement is available from strategic communications, provide the below message to staff receiving calls to use until a statement or talking points are made available:

"Thank you for reaching out about this issue. Our team is aware of the situation. All inquiries and questions about this are being handled by Strategic Communications."

If the attack is impacting an instructor, prepare if, when and how questions about how the situation will be addressed with their students. Keep in mind that if the attacks are threatening in nature and are public, some students may feel uncomfortable coming to a classroom. Have a plan to move the class location, offer remote options, or take other appropriate steps. Think about whether the impact of the attack ripples out to other classrooms, labs or others in your department. Create a contingency plan to take effect if the issue persists long enough to impact the instructor's ability to teach effectively. Consider options (such as bringing in substitutes or creating other ways to cover the curriculum) to keep classes moving forward.

PART THREE

Tips to Help Safeguard Your Social Media Engagement (Nested in Social Media Guidelines)

Tips to Help Safeguard Your Social Media Engagment

Tip One. Avoid using your full name.

Avoid creating social media handles that have your full first, middle and last names. If using social media to advance your professional career, consider just revealing your first and last name and not revealing your middle or other surnames.

Tip Two. Regularly review your privacy settings.

Social media platforms all have privacy settings. These settings give you the power to choose who can see your profile, who can message you, who can tag you and how much information is shared from social media publicly. Each platform is different and privacy settings can change frequently. Consider privacy settings as a regular maintenance task that needs to be checked on at least once a year. Visit the specific social media sites for the most up to date information.

Tip Three. Do not post personally identifiable information.

Don't post information that can help identify your address, office, your license plate or other personally identifiable information. Some of this information can be less obvious — check the background of images for mail, your address, ID numbers, sticky notes with passwords, notebooks, etc.

This also includes not posting proprietary information that can be found in documents, white boards and in the backgrounds of some research labs or offices.

Tip Four. Don't post about your whereabouts until after you've left.

Your location is vital information about you. Don't post about trips until after you've returned.

Tip Five. Change your passwords often and set up two factor authentication.

Take full advantage of the extra security measures of two factor authentication and change your passwords frequently.

Tip Six. Only follow accounts that you know are credible and are trustworthy.

Be judicious about who you follow back on social media. Take the time to make sure it is a real account run by an actual person and not a bot. This also applies to content that you share — take the time to ensure it's from a credible source and click beyond the headline before pressing share.

Tip Seven. Build your support network and ground your own reputation.

Connect with colleagues, peers, mentors, and leaders and contacts online. Be active with this group and support them. Chances are if you ask your support network for help, they will reciprocate.

Tip Eight. Take the high ground and don't feed the trolls.

Trolls thrive on conflict and in general are not online to listen to reason. Don't give them the satisfaction of engaging in debate. Take a break before engaging or replying and use this litmus test "would I be proud if this post/reply was published by [insert huge media company here]?" If the answer is no, don't post it. You can always get a gut check from a friend.

Tip Nine. Use your voice

In some rare circumstances, it is appropriate to use your personal social media channels to share your side of the story. Before you consider this approach, take your time to evaluate the online conversation, your stance and what you want to say. Ask for several gut checks from peers and from your department leaders before posting. Avoid the temptation to rush into responding. Sometimes this step has potential for massive backlash — so engage with extreme caution. More often than not, this step isn't necessary as the issues blow over faster than most expect.

Tip Ten. Block, mute, and report without remorse.

All social media platforms have the ability to block users from accessing your social media content or being able to direct message you. If someone is leaving you unwanted messages, comments or tagging you on your own social media posts or pages hit that block button!

You do not owe anyone an explanation about why you've blocked or unfriended them.

If blocking is too harsh, Facebook, Twitter and Instagram have "mute" options that can silence notifications from an individual or cut out those conversation threads that you don't want to see without blocking.

Report users and profiles who are engaging in harassing behaviors, making threats or are impersonating you directly to the social media platform. Most platforms act quickly on these reports as it is against the terms and conditions of use and once verified that the offending actions are against harassment policies, user comments and accounts can be deleted. In extreme cases, users can be banned outright from using the platforms. These reports are also used for any police case filings or warrants.

Tip Eleven. Visit our page for more resources if you think you are experiencing online harassment.

communicationsguide.ucdavis.edu/departments/social-media/policy-and-guidelines/trolling-guide/checklist

WHERE DO I GO FOR HELP?

If you're looking for resources or have questions about the brand, please contact us via one of these channels.

Brand Guide: brandguide.ucdavis.edu

Social: socialguide.ucdavis.edu

Web: webguide.ucdavis.edu

Video and Photography: photovideoguide.ucdavis.edu

News: newsguide.ucdavis.edu

Executive Communications: executiveguide.ucdavis.edu

Trademark Licensing: trademarks.ucdavis.edu

For help or office hours scheduling:

email: socialmedia@ucdavis.edu

Slack: @social_braintrust

MAY 12, 2023

UC DAVIS

ucdavis.edu