Guide To Addressing and Combatting

ONLINE HARASSMENT

Salisbury UNIVERSITY

CONTENTS

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 unsolicited sexual messages or images.

Actions to Take if You Are the Target of Online Harassment

Actions to Take if You Are the Target of Online Harassment

1 *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 SU Police Department (410-543-6222).

2 *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, supervisor, IT, case workers or police units who may be assisting you and could be used as evidence.

3 *Get Support.*

For faculty. Connect with your administrative leader (department chair, program director, the dean's office).

For staff and student employees. Reach out and alert your supervisor right away, especially if the harassment may be in relation to your work.

If the harassment is gender-based harassment and/or sexual in nature, consult the Title IX Coordinator to understand your rights and resources.

If the harassment is based on another protected class (e.g., race, age), consult with the Office of Institutional Equity to understand your rights and resources.

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 SU Public Relations Office (410-543-6030), who will help you sort through the next steps.

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. Employees should work with campus Human Resources and the Web Development Office for help with website/directory listings. 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.

4 *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.

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, X 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. 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 – contact Integrated Marketing for help with this).

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.

Checklist for Academic Leaders and Supervisors Supporting Employees Experiencing Online Harassment

Checklist for Academic Leaders and Supervisors Supporting Employees 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 employees who are impacted.

1 *Evaluate If Immediate Action Is Needed.*

CALL 911 IF YOU FEEL THE EMPLOYEE, THEIR FAMILY OR AN IDENTIFIABLE GROUP (FOR EXAMPLE, A CLASS) ARE IN IMMINENT DANGER.

See roles, actions and resources in Step Five for situations that are serious, but harm is not imminent.

2 *Provide Resources.*

Share with the employee the link to this page so they can review the "Actions to Take if You Are a Target of Online Harassment" guidance (if they have not done so already).

3 *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.

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.

4 *Confirm that the SU Police Department Has Been Contacted.*

If not, do so immediately. Provide whatever documentation you have collected so far to the Police Department and to other responding units as directed. See additional roles, actions and resources in Step Five.

5 *Understand Roles, Actions and Resources and Mobilize As Needed.*

In matters of safety and security, employees are encouraged to make use of campus resources to assist them in responding to an immediate situation, as well as to address any concerns that arise in the longer term. Numerous campus resources are also available to support department chairs, supervisors and college administrators in responding to external attacks of SU employees. Knowing about relevant resources and guidance in advance of a crisis will help our campus respond more effectively when a situation arises.

In an emergency, call 911. In non-emergency situations, please call the SU Police Department at 410-543-6222.

The following offers suggested actions and resources for individuals in various roles at the University, including:

- Department Chair/Program Director
- Dean/Associate Dean
- Marketing and Communications Staff
- Provost's Office (For Faculty Incidents)

Department Chair/Program Director/ Unit Supervisor ⟩

- Contact the faculty member as soon as you become aware of the situation. Meet with them to offer support in the initial days after the attack and review the "Actions to Take if You Are a Target of Online Harassment" guidance on this page to ensure the faculty member is aware of campus resources.
- If not already done, report the situation to SU Police Department, which is trained to assess these situations and assist with coordinated responses, as needed. Also consult with the Public Relations Office if the situation warrants it.
- Before all else, work with the faculty member to ensure that their on-campus and off-campus safety and security concerns are addressed in consultation with SU Police Department. Be aware that the identity of the faculty member may influence their individualized needs (e.g., parental status, faculty rank, minoritized identity). With the faculty member's consent, reach out to appropriate campus resources to address whatever issues the faculty member identifies.
- Report the situation to your dean.
- It is important to work with SU Police so they are able to assess risk and determine the best course of action. Below are some possible actions that may be advised under their guidance – such actions will be advised on a case-specific basis (to ensure de-escalation of a situation, rather than escalation):
  - Inform the department/office administrative staff on a need-to- know basis. It is possible that multiple offices may be targeted on social media, email or phone. Ensure that staff members whose responsibilities may include answering harassing phone calls are supported and informed about strategies for being on the front line (e.g., a script or template response, instructions for preserving phone messages to aid future investigations) – see suggested first response language in Step 6 below.
  - Stay in communication with your dean's office to ensure a coordinated response. Share details of the situation on a need-to-know basis and be mindful that communications may be subject to disclosure pursuant to a public records request.
  - Consider the well-being of the rest of the department/office faculty, staff and students (e.g., co-authors, graduate assistants, front-line staff). Consult with the threatened employee about what and how to share information with the department/office. If possible, bring people together to discuss the situation, the department/ office's actions and available support resources.
  - Facilitate the physical movement of assigned classrooms and/or workspace if feasible, and if the affected employee requests it.
  - At the affected employee's request, facilitate the removal of the their direct contact information from SU webpages, including directory, in collaboration with Human Resources and the Web Development Office.
- If the harassment is gender-based harassment and/or sexual in nature, promptly consult the Title IX Coordinator to ensure that the faculty member is fully aware of their rights and resources.
- If the harassment is based on another protected class (e.g., race, age), consult with the Office of Institutional Equity to counsel the employee about their rights and to explore additional support options for the employee and others in the department who share their identity (e.g., students, colleagues, staff).
- After addressing the employee's safety and security concerns, keep in mind the potential impact of this event on their academic career. For example, if their scholarship was attacked, discuss any concerns the faculty member has about how/whether it will affect their future research trajectory. Connecting the faculty member with other scholars who have experienced similar attacks may be useful to contextualize the events within their broader career goals and experiences.

- Discuss issues of academic freedom in regular forums (e.g., faculty meetings, student seminars), including attention to ways that external forces may attempt to silence scholars through social media attacks and the resources available to respond when/if attacks occur.
- If you become the target of harassment, consult with the dean's office and refer to the strategies recommended for employees (above) to ensure your own safety.

Dean/Associate Dean ⟩

- Proactively develop a leadership message that defends academic freedom, the importance of faculty safety, and the development of learning environments in which difficult issues are discussed and dissected to use as a template should these types of crises emerge. Work with the Public Relations Office to develop a message that emphasizes University values, draws upon best practice examples from other campuses and addresses potential concerns of multiple constituents (e.g., faculty, alumni, legislators, donors, students).
- Engage school/college leadership in coordinating the college-wide response, including support for staff who may be experiencing stress due to being on the front line of answering harassing phone calls and/or may be concerned about their own safety.
- If a crisis emerges, consult with the targeted faculty member and the Public Relations Office to share how you would like to publicly handle the crisis and discuss any concerns they might have. Involve the faculty member's department chair in crisis management conversations to ensure that efforts are coordinated.
- Support the department chair in working with the targeted faculty member by offering assistance and resources. See "Actions to Take if You Are the Target of Online Harassment" above to ensure that the targeted faculty member's immediate and longer-term needs are cared for.
- Inform the dean's office staff on a need-to-know basis. It is likely that social media and phone harassment will be directed at multiple offices. Informing all relevant individuals in the dean's office will strengthen the college's ability to engage in a coordinated response. Ensure that dean's office staff members whose responsibilities may include answering harassing phone calls are supported and informed about strategies for being on the front line (e.g., a script or template response, instructions for preserving phone messages to aid future investigations) – see suggested first response language in Step 6 below.
- Be aware that other faculty and staff, as well as students, who share the research area under attack may also experience significant emotional distress because of the incident.
- Depending on the nature of the attacks, be aware that students, staff and faculty who share the identity may also be personally experiencing significant emotional distress because of this incident.
- Consult with the Office of Institutional Equity, Human Resources (for employees) and the Counseling Center (for students) to arrange for support services for students and staff in the school/college, if needed.

Marketing and Communications Staff ⟩

- Inform the dean if you become aware that an employee's name has shown up in a harassing social media post (e.g., via a Google Alert notification). Keep the dean informed of ongoing mentions throughout the crisis management process.
- Work with the dean's office and other campus spokespeople to coordinate information sharing on a need-to-know basis and to coordinate a consistent message (e.g., phone scripts for front-line staff answering aggressive callers).
- Consult with faculty, staff and administrators about media policy and the potential impact of speaking with the media about faculty harassment.
- Offer media training and guidance.
- With the deputy chief of staff for communications, provide assistance to schools/colleges in crafting a leadership message that defends academic freedom, emphasizes university values, and addresses potential concerns of multiple constituents (e.g., faculty, alumni, legislators, donors, students).

Provost's Office (For Faculty Incidents) ⟩

- Establish open communication with the affected faculty member's dean and request updates, as needed, on the situation.
- Reach out to the targeted faculty member, reiterating the University's commitment to academic freedom (as appropriate) and encouraging the faculty member to consult with their department chair for support and assistance.
- In consultation with the Office of the President and Public Relations Office, issue a statement (as appropriate) asserting the importance of academic freedom, freedom of speech and committing to the safety of the faculty. The statement should emphasize the institution's mission and values rather than comment on the faculty member's scholarship.

6 *Prepare Teams for Potential Impacts.*

Prepare staff to handle phone calls, emails, social media comments and inquiries about the harassment issue. The Public Relations Office can provide an approved statement upon request. If no approved statement is immediately available, 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 the SU Public Relations Office."

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 and 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.

Tips to Help Safeguard Your Social Media Engagement

Tips to Help Safeguard Your Social Media Engagement

1 *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.

2 *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.

3 *Do not post personally identifiable information.*

Don't post information that can help identify your address, office, 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, on white boards and in the backgrounds of some research labs or offices.

4 *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.

5 *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.

6 *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.

7 *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.

8 *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.

9 *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, and inform the Public Relations Office in preparation for any additional fallout. 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.

10 *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, X 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 these actions are against the terms and conditions of use. 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.

Salisbury University

Make Tomorrow Yours

This guide was created, with permission, from excerpts adapted for Salisbury University from the University of California, Davis' "Guide to Combatting Social Media Trolls and Online Harassment" and Boise State University's "Faculty Support and Resources Guide."