



As members of the University community, it is our responsibility to maintain a culture of respect and inclusion in our online spaces.

What is online abuse?

Electronic, online or “trolling” attacks or abuse can take many forms, including online threats or unwelcome messages or images, cyberstalking, or attempts to hack or shut down accounts.

What are some proactive steps I can take to avoid online abuse?

- Increase your awareness of commonly-used symbols, signs, euphemisms and phrasing; one helpful resource is the Anti-Defamation League’s [Hate Symbol Database](#).
- Familiarize yourself with your platform’s (e.g. Zoom) online forum security settings.
- Use available restrictions and follow best practice guidelines.
- Establish ground rules with students regarding online respect.
- Practice basic cybersecurity and personal information security.

Source: [PEN America Webinar: 'What Professors Need to Know About Online Harassment'](#)

What are some steps I can take to secure asynchronous online spaces?

You may be using online spaces like discussion boards. Below are some steps to take to protect those spaces from online abuse:

- Post “Rules of Engagement” for the online platform, emphasizing respectful interactions.
- Familiarize yourself with how to report abusive users, including users of fake profiles.
- Closely monitor online content to flag any potential cases of online abuse.
- Phone the [Office of Institutional Equity and Diversity](#) for nuanced advice on what constitutes free speech vs. hate speech in academic settings.

Source: [McGraw Center for Teaching & Learning](#)

Tips to Secure Your Zoom Sessions

(click the bolded text for more information)

- **Require registration:** This shows you the email addresses of everyone signed up to join your class, which can help you evaluate who is attending.
- **Use a random meeting ID:** Generating a random meeting ID is the better alternative to using your *Personal Meeting ID* (which essentially creates an ongoing meeting).
- **Password-protect the classroom:** Create a password for each meeting and share it with your students via their Princeton University email so that only those intended to join can access the virtual classroom.
- **Allow only authenticated users to join:** Checking this box enables only designated users who are signed into their Zoom accounts to access a particular class.
- **Disable join before host:** This ensures that students cannot join class before you join; they will see a pop-up saying, “The meeting is waiting for the host to join.”
- **Control screen sharing:** Zoom’s sharing privileges are set by default to “Host Only” so that only you can share content in class. If students need to share work with the group, you can allow screen sharing using the host controls.
- **Manage annotation:** Disable participant annotation in the screen sharing controls to prevent students from annotating on a shared screen and disrupting class.

Source: [Zoom](#)

Questions? Contact the Office of Institutional Equity & Diversity by emailing bias@princeton.edu.

How do I respond to online abuse?

If your online platform is disrupted by online abuse (i.e., “Zoombombed”), we recommend taking the following immediate eight steps:

1. Take an immediate screenshot of your screen.
2. Calmly acknowledge what is happening to your students.
3. Ask all participants to pause their videos immediately.
4. Utilize your online platform’s settings (if using Zoom, use the “Speaker View” feature) to identify the user and remove that participant from the Participant Box.

If you feel that you or others are in immediate danger, call 911 and report the issue immediately. If possible, follow this up with a call to the Princeton University Department of Public Safety at 609-258-1000.

Once the disruptive user(s) have been removed from the online space, we recommend that you:

5. Acknowledge clearly that what happened was unacceptable, and affirm Princeton’s commitment to respect.
6. Continue with your planned session.
7. Before the session ends, download the Zoom Chat and take screenshots of any other records used during the online activity.
8. Follow up with the Office of Institutional Equity & Diversity by emailing bias@princeton.edu.

Email Template:

Sample text (to be personalized/modified as appropriate):

Dear [STUDENTS],

I’m sorry that we/you all had to encounter a distressing incident online today. As all members of the campus community are encouraged to report bias incidents, I’ve reported this matter to the University at bias@princeton.edu, and I encourage you to report this incident to Public Safety at 609-258-1000.

If you and/or others who were impacted by this incident are in need of additional support, it may be helpful to seek confidential campus resources: Counseling and Psychological Services (<http://uhs.princeton.edu/counseling-psychological-services>), Office of Religious Life Chaplains (<http://religiouslife.princeton.edu>), Ombuds Office (<http://princeton.edu/ombuds>), SHARE (<http://share.princeton.edu>), and the Carebridge Employee Assistance Program at 800-437-0911 (for graduate students and employees). Additionally, you might also wish to seek support from on-campus [non-confidential campus resources](#).

Questions? Contact the Office of Institutional Equity & Diversity by emailing bias@princeton.edu.

Asynchronous Online Spaces (such as discussion boards or online forums)?

- Take a screenshot of the full thread.
- Make a short comment in the forum that this material is unacceptable.
- Use your best judgement regarding whether the material should be deleted (it should not be deleted if it is potentially protected free speech by a student). *If you are unsure, contact bias@princeton.edu for advice.*
- Make a written follow-up statement to your class using clear, noninflammatory language to inform your students that you are aware of the content and that it was inappropriate. **A template for crafting this email is available below.**
- Follow up with the Office of Institutional Equity & Diversity by emailing bias@princeton.edu.

What are the next steps?

Refer students who have been impacted by online abuse to appropriate University resources for additional support, including:

Confidential Resources: Counseling and Psychological Services (CPS), Office of Religious Life chaplains, SHARE, Ombuds Office

Additional Resources: Directors of Student Life, Graduate School, LGBT Center, Carl A. Fields Center, Women’s Center, Carebridge Corporation (Graduate students and employees only), Davis International Center