UC DAVIS
UNIVERSITY OF CALIFORNIA

FAQs on Privacy in Zoom Classrooms

Draft Publication Date: 9/21/2020

FAQs on Privacy in Zoom Classrooms[1]

1. Has the campus assessed Zoom's privacy policy or other contractual commitments?
2. What are the top 10 things I can do to protect the privacy of my Zoom sessions?
3. What do I do if I am Zoombombed or if my Zoom session is hijacked?
4. Is it better to use the web app or download and use the Zoom app?
5. What is recommended to protect the privacy of my students and myself? Do you have "remote classroom etiquette" sample language?
6. What if I want to require all of my students to have their video on?
7. How do I create and keep a Zoom "channel" private?
8. Are there privacy concerns related to the recording of lectures? How can I protect my faculty Intellectual Property (IP) rights with recorded Zoom lectures? If I want to avoid recording and yet make my courses available asynchronously, what alternatives do I have?
9. What privacy laws and policies may apply to my Zoom sessions?
10. Who should I contact for help on Zoom or questions about this FAQ?
11. What about general privacy and remote teaching concerns (not just limited to the Zoom platform)? What if I would like to recommend a change to these FAQs?

Note: These FAQs are intended for faculty and instructors who use Zoom for teaching on the main campus. These FAQs are not intended for guidance on non-teaching Zoom uses or for use of UC Davis Health's Zoom, a separate program. These FAQs are also not intended for remote exam proctoring.

Acknowledgements: We would like to thank Dean Cynthia Ching, Professor Matt Bishop, and Professor Elizabeth Joh for their review and comments. We also greatly appreciate comments from our colleagues at the Office of Student Support and Judicial Affairs, the Center for Educational Effectiveness, and the Student Disability Accommodation Center. Finally, we are grateful for contributions from the Information Security Office who co-developed earlier versions of a portion of these FAQs published in the summer of 2020.

[1] This privacy guidance is not intended for use of Zoom in remote exam proctoring situations. A separate guidance document will be developed by the Privacy Office for remote exam proctoring and privacy concerns.

FAQ Answers

1. **Has the campus assessed Zoom's privacy policy or other contractual commitments?**

   Yes, the UC Davis Privacy Office reviewed Zoom as a part of the UC Davis Information Security Office vendor risk assessment and found that the third-party privacy review while likely still valid, could benefit from an updated 2020 review. The UC Davis Information Security Office has requested an updated report from Zoom.

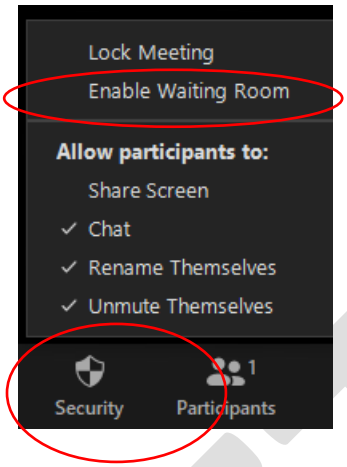
   Zoom's current Privacy Policy commits to never selling customer information and to not using customer data stored on the Zoom app for advertising. Zoom's Privacy Policy also states that Zoom "collects only the user data that is required to provide you Zoom services."

   Additionally, under the University of California (UC) systemwide contract with Zoom, Zoom is contractually bound to not sell your data to third parties and not use your non-public data for any purpose other than to carry out UC's purposes. The contract prohibits Zoom from using UC's non-public information for Zoom's own benefit. Non-public information as defined in the contract includes: information that identifies or is capable of identifying a specific individual, information that is marked or identified as proprietary or confidential, information that can reasonably understood as confidential, business information.

   For more information on Zoom's privacy assurances, see the April 20, 2020 webinar that Zoom gave to members of the higher education community that addressed privacy concerns. Additional information is available here. Zoom has also provided additional guidance to education community on April 24, 2020 through a blog post available here.

2. **What are the top 10 things I can do to protect the privacy of my Zoom classroom sessions?**

   1) Use the most current version of Zoom (see How do I update my Zoom application).
   2) Do not post Zoom links or invites on social media or public websites (see How to Secure the Zoom Meeting Information section 2.7);
   3) Use a unique ID for each meeting instead of using your Personal Meeting ID or PMI (see How to Control who can join your meeting, section 2.2);
   4) Use meeting passwords (see How to Control who can join your meeting, section 2.1);
   5) Avoid recording or practice "secure" recording; if you must record, password-protect the recording, rename the saved recording, save it on Aggie Video (not Canvas or Zoom) (see How do I secure my Zoom Recording); remember to notify students in advance and offer an opt-out alternative.
   6) Turn off embed password in meeting link (if applicable). This will require users to type in a password rather than have one click access. (see How to Disable Embed password in meeting link, section 2.5);
   7) Enable Waiting Rooms and have the host allow users in one by one, or all at the same time, once all attendees have been verified (see How to Use a Waiting Room, section 2.6);



8) Lock meetings once all participants have joined, if applicable (see How to Secure the Zoom Meeting Information, section 2.7);
9) Disable file transfer settings during zoom meetings (see How to Control what participants can do in your meeting, section 3.4);
10) Contact your Zoom instance administrator. Each College at UC Davis has one administrator. See here for their contact info.

Once you've mastered the top 10, here are a few additional tips to consider:

- Zoom has additional recommendations on its privacy and security page and best practices for securing your virtual classroom. Note: Some recommendations on Zoom's page may not apply to you; we have attempted to extract top tips that apply to UC Davis in FAQ#1 above. For example, Zoom recommends restricting meeting participants to those who are logged into Zoom or those in your domain (e.g. UC Davis email addresses). However, this feature (restricting meeting participants to UC Davis emails) may not work for all undergraduate teaching Zoom users.
- Require advance meeting registration for large meetings, or non-instruction sessions (e.g., webinars) where the audience is not predetermined. Guidance on how to set up meetings that require registration is available here.
- Consider updating your Zoom default settings. Guidance on recommended default settings is available here. Your college's Zoom instance administrator may have already updated them for you.

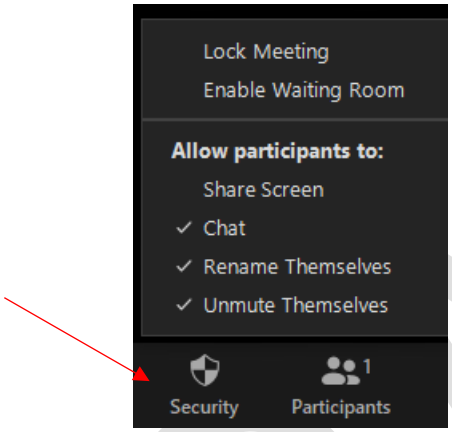
3. What do I do if I am Zoombombed or if my Zoom session is hijacked?

Zoom sessions that are not password protected can be hijacked by invited individuals or joined by uninvited individual(s). Zoombombing, a type of cyberattack, is where an individual(s) would enter a Zoom meeting and broadcast obscenities or take unauthorized control of the screen.

Here's what to do, if you're Zoombombed:

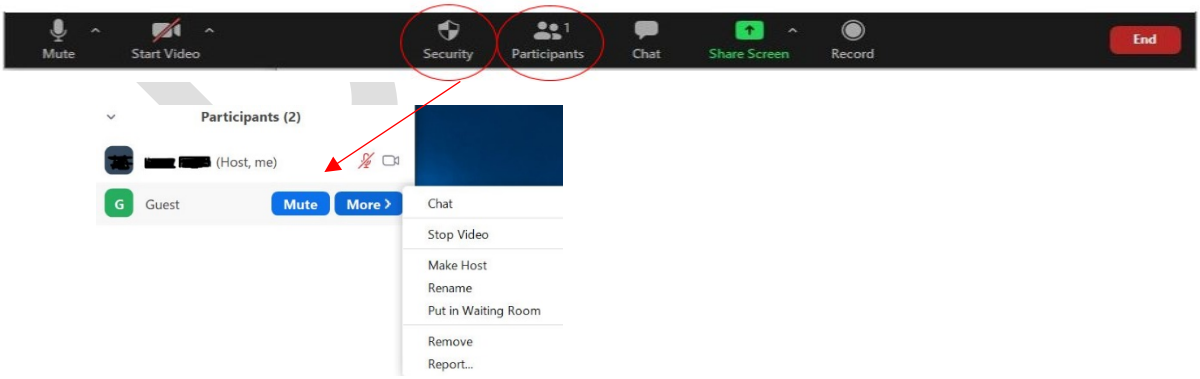
Use the Zoom "Security" icon found on the toolbar to stop access:
*Information on controlling security features on non-PC operating systems is here.

- Lock the meeting
- Enable the Waiting Room (if it's not already enabled)
- Restrict participants' ability to:
  - Chat in a meeting
  - Rename themselves
  - Unmute themselves
  - Share their screens [For education users, sharing privileges are now set to "Host Only," so instructors by default should be the only ones who can share content in class. If an instructor turns on participant share, do so carefully.]



Use the "Participant" icon to further restrict access:

- Disable or Stop Video
- Mute participants
- Mute all (disable allow participants to unmute themselves)
- Remove participants



If Zoombombing happens to you, call the IT Express Desk at 530-754-HELP who can put you in touch with your Unit IT Lead or contact your Unit IT lead. See here for a list of Unit IT leads.

Once you contact IT staff, they will notify other appropriate campus authorities including the Campus Information Security Office, cybersecurity@ucdavis.edu, and the Campus Privacy Office, privacy@ucdavis.edu. The Campus Information Security Office and Campus Privacy Office may engage the UC Davis Police Department accordingly. Zoombombing is considered a cybercrime, and UC Davis Police may report the incident to the FBI.

4. Is it better to use the web app or download and use the Zoom app?

Zoom's Chief Privacy Officer claims that there is no difference in privacy levels between using the web application versus using a downloaded application. The sole difference described by Zoom's Chief Privacy Officer is that the user may need to manually download the latest version, whereas the web application automatically updates.

If you are using the desktop client, you should regularly check and install the latest Zoom updates. Or, check with your local IT administrator, who may have already programmed automatic updates for you. Guidance on how to update your Zoom app is available here.

5. What precautions are recommended to protect the privacy of my students and myself? Do you have "remote classroom etiquette" sample language?

This section includes recommendations to protect privacy in remote classrooms. These principles apply to protecting the privacy of students from other students, students from faculty, and faculty from students. Instructors should consider developing Zoom classroom etiquette or remote classroom code of conduct guidelines for students, including considerations protective of individuals' privacy rights. The principles can be placed in your syllabus, with periodic visual notice reminders to students at the beginning of each class session.

(a) Remote Classroom Etiquette Sample Language and Tips

Below is some sample language for instructor consideration. [Note: This sample language is for conducting class on Zoom and is *not* intended for use of Zoom in remote exam proctoring situations, which will be the topic of a separate guidance document.]

- Sample Language on the UC Davis Code of Academic Conduct:

  "As a member of the UC Davis community, students are expected to adhere to the UC Davis Code of Academic Conduct that supports high standards of behavior and ensures fair evaluation of student learning."

  Note: The Office of Student Judicial Affairs has suggested course syllabi language to help instructors reduce the likelihood of cheating. For more information, contact ossja@ucdavis.edu or check their syllabus suggestions website.

- Sample Language on Privacy Generally and Capture, Use, Distribution of Zoom Content:

"Respect for privacy is an essential part of our classroom community. Images, text, screenshots, audio/video content from Zoom sessions may only be used for instructional purposes of this course. Participants should not distribute data captured from Zoom sessions to anyone outside the course, without appropriate consent from the individuals whose images/voice/data are involved. Unauthorized distribution or capture outside the course may violate federal or state privacy laws or University of California policies. This means, for instance, you should not post screenshots of your class, your instructor, or your classmates to social media."

- Sample language on recording Zoom classroom sessions:

  "Recording is only permitted by the instructor, by Letter of Accommodation issued by the Student Disability Center, or with instructor approval. If recording, the instructor will provide advance notice to participants of an intent to record a session, with an opportunity for students to petition the instructors for an opt-out of video/audio participation. Opt-out requests will be granted at the discretion of the instructor or a campus-designated office, only if the students demonstrate a reasonable basis for declining video or other participation."

  While students should seek instructor approval before recording a course, instructors are encouraged to be flexible in granting recording requests and also reasonable in allowing students to opt-out of video/audio, if sessions are recorded. Recording may be required as a reasonable accommodation for some. Other students with histories of abuse or post-traumatic stress have reported being psychologically triggered when watched by a camera in their homes and may need to request a video/audio opt-out when being recorded. Or, recording and asynchronous access may be important due to time zone differences, caretaking responsibilities, or challenging home environments.

  If an instructor records their own course and makes it available to students for a limited duration, you better control the security of that recording (e.g. storing the recording on secure University software (such as Aggie Video) which does not permit downloading). Instructors may also minimize the risk of insecure self-help methods such as students recording a lecture on their own devices. (You can also minimize the risk of self-help by reminding students that unauthorized recording is contrary to University policy and the Academic Code of Conduct.)

- Sample Language on Privacy of Chats:

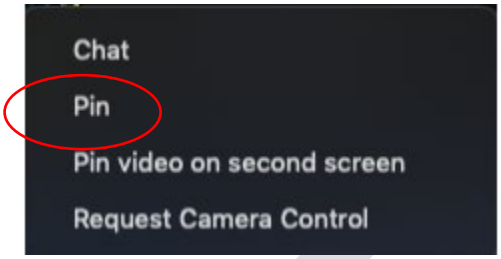
  "Students should not save or record classroom chat exchanges, including photographing, screen capture, or privately saving chat exchanges, without explicit instructor permission."

  Alternatively, faculty may want to advise students that their text chats may not be private. Any user may save chat comments sent to "everyone" as a file on their computer. Private text chats may also be saved (as a file) by the intended recipient(s) of that text chat. You may want to consider turning "off" the private chat function.

- Sample Language on Pinning / Furtive Surveillance

*"Students should not pin the image of another classroom participant, without their knowledge or consent. This may be invasive of their privacy and, in some cases, could be considered harassment." See ** note below.*

Pinning allows participants to magnify and "watch" the image of another person in the Zoom room, without that person's knowledge. This may constitute harassment.



Zoom typically defaults to "speaker" view, but pinning allows you to watch and magnify someone else, the person of your choice. While there are legitimate purposes for pinning (i.e. sign language interpreters), students could be reminded that pinning can be extraordinarily invasive of another's privacy rights, as it is close-up surveillance of another without their knowledge. More information on pinning is available here.

** Note: While sample syllabus language on pinning is provided here, instructors should also consider whether including the language may draw students' attention to pinning, potentially worsening the problem. Some believe that many if not most students are already aware of this feature – so, we have included this language for consideration.

– Sample Language for Emergency Arrangements on Zoom.

"Emergency arrangements policy. If you suddenly need to turn off your video/audio, your video/audio access is suddenly interrupted, or you cannot log into a class, notify the instructor immediately by either [insert one communication medium, e.g. send an email, leave a voicemail, etc.] so that the absence may be excused."

Some students may have legitimate reasons for non-video, non-audio, or non-personally identifiable participation. These reasons could range from privacy concerns, due to past incidents or current harassment, or technological constraints related to limited bandwidth or computer capacity.

Consider posting a plan B, and advise students on how they should notify you if technological (bandwidth or internet connection) or privacy constraints (sudden family incident or interruption in the background) suddenly arise before or during class, which preclude video/audio or other participation or require being temporarily offline. For example, advise students how you prefer to be notified (email, chat, Canvas, etc.). Consider allowing easy access to a plan B (course on Canvas; or access to asynchronous recording), etc.

- Sample Language on Alternative Arrangements:

  Some students may consistently not be able to participate via video or internet. Consider informing students of the opportunity to seek approval for an alternative arrangement.

  "Alternative Zoom arrangements policy. If students have serious privacy, safety, or other concerns or technological/bandwidth constraints, students must arrange in advance to address these concerns with their instructor or by Letter of Accommodation. With instructor approval, alternative arrangements such as audio only may be permitted."

  Sample alternative arrangements include:

  - Audio-only participation as an alternative to video to minimize bandwidth usage.
  - Using an appropriate virtual background if they do not want to have their surroundings visible (this feature is not available for all Zoom instances and may cause video quality issues). More Zoom info is here.
  - Allowing a student to not use their photo;
  - Allowing a student to use an alternative to their full name, such as the student's initials, the student's first name, or last name only.

  All alternative arrangements should be pre-approved by the instructor and should still allow the instructor to identify the student. For privacy, the student need not divulge the reason for the request (e.g., I'm a sexual harassment victim, etc.). To provide accommodations and ensure privacy of students with disabilities, a Zoom breakout room can be created. More information is available here. With the exception of Letters of Accommodation, alternative arrangements may not be possible for remote exam proctoring. Please see remote proctoring and privacy guidance on the campus privacy page. The remote proctoring guidance was issued in May 2020 and will be revised during the Fall 2020.

- Limits of Sample Language for Syllabi / Not for Remote Proctoring

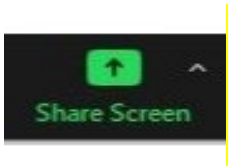
  "This guidance is not intended for remote exam proctoring, which has unique constraints and needs. Separate guidance specific to remote exam proctoring needs may be provided by your instructor."

(b) Additional Considerations for Instructors:

Remote teaching creates opportunities for students to inadvertently view your private home or location background or your private digital information and history. Here are a few technical safeguards to consider to protect your own privacy:

- Consider programming Zoom so that "Video off" is your default when you turn Zoom on. Otherwise, students may inadvertently view your background, as you are setting up your classroom or background.

– Before sharing your screen, close open files, emails, browser tabs, and browser bookmarks bar. Turn off pop-up email or reminder functions so that they are not viewable when you are sharing your screen. Be mindful that when you enter information in a search bar, while screen sharing, students may see your recent search history. If you enable screen share by students, remind them to take the same precautions.



6. What if I want to require all of my students to have their video on?

Requiring students to turn on their camera and to be recorded poses privacy concerns and should be undertaken with care and transparency. We recommend that instructors exhaust feasible alternatives prior to requiring video be turned on and advise students of potential alternatives in advance. See FAQ#5 above for potential alternative arrangements and recommendations for protecting student privacy.

Below are examples of challenges that may affect their ability to comply with video-on mandates or where they may raise privacy concerns:

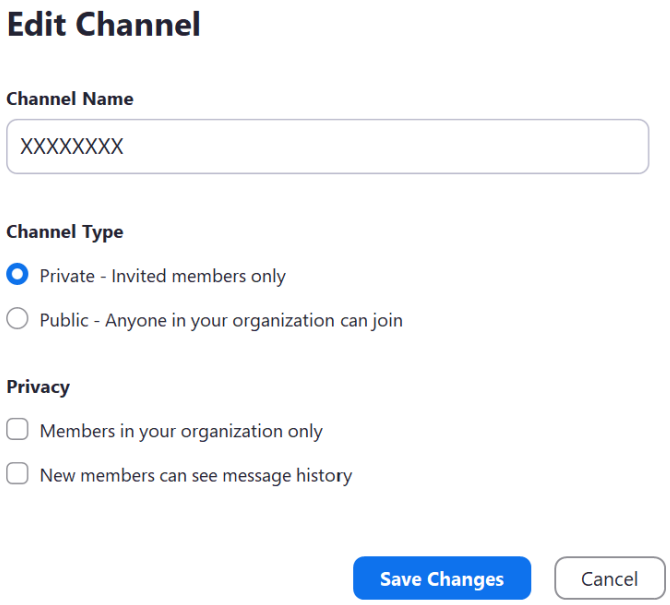
- Access to technology or equipment: inability to pay internet bill, low-tech environment, poor internet connectivity, low bandwidth, or limited computer hardware.
- Private space or environment: chaotic home environment, concern over judgement of private space, view of personal bedroom or space, limited or no access to private space.
- Video recordings has been reported by some students in the UC to trigger a prior history of abuse or post-traumatic stress disorder.
- Misuse of or unauthorized access: sharing video, screen captures, or photos; pinning (allows participants to magnify and "watch" the image of another person in the Zoom room, without that person's knowledge. More information on pinning is available in FAQ#5 above and here).

Note that video alternatives may not be possible for remote proctoring situations. We suggest different alternatives for remote proctoring. See here.

7. How do I create and keep a Zoom "channel" private?

A Zoom channel can help with your Zoom teaching by creating a "chat room" or virtual bulletin board that all class members (including the instructors) have access to outside of normal class hours. Information on how to create a "class channel" is available here.

Zoom has updated privacy controls for a channel. You can view your privacy controls, control who can view past channel chats, and control whether the channel is private or public, as displayed in the below graphic.



By selecting "Members in your organization only" (displayed in the icon above), only UC Davis members can be added to the channel. By selecting "New members can see message history" (displayed on the icon above), newly added members to your channel will be able to see all the messages in the channel including those that were written before the new member was added. More guidance on creating and using channels group messaging is available here.

8. Are there privacy concerns related to the recording of lectures? How can I protect my faculty Intellectual Property (IP) rights with recorded Zoom lectures?

Safe storage of recorded lectures:
We encourage faculty to avoid the "publish" link in Zoom, as it is shareable and can be re-posted on a public website. Instead, faculty are encouraged to use Aggie Video (not Canvas) to store video recordings, and share lectures with students (see How to save a Zoom Cloud recording to Aggie Video and embed into Canvas), which allows sharing to be limited to UC Davis.

The Campus Information Security Office has evaluated the security controls around videos uploaded in Canvas as files and determined that Canvas does not have sufficient controls to ensure privacy of information in the video recording. When you upload a video recording to Canvas and a student downloads it, you have no control on what the student can do with the video. Aggie Video gives the instructor more controls on what the student can do with the video.

As an additional precaution, instructors can disallow viewers from downloading video files to their own computers by turning off the "Viewers can download" option in the sharing settings for recordings stored in Zoom's cloud. With this option disabled, viewers can only view the video in a web browser and not download the actual video files. This makes it harder for viewers to

intentionally or accidentally re-share videos. More information on the sharing options for Zoom recordings is available here.

Post a Recording Notice:
To protect the privacy of your students and lectures, check that your Zoom instance administrator has programmed the pop-up notice. The notice should advise all participants of the recording and of recording rules, rights, and restrictions.

Below is a sample video recording disclosure message:

"This session and any personal information you share during the session will be recorded. Participants are prohibited from electronically capturing or re-disclosing session information. Participants may opt-out of being personally identified only with advance host/instructor approval."

Offer an Opt-Out Option to Students:
Prior to recording a lecture, also notify students in advance that sessions will be recorded and that students may opt for privacy-protective alternatives, with instructor approval.

Campus Zoom accounts do not have the security levels to store personal health information, therefore, any meetings that contain this information should not be recorded.

Limit Retention period for course recordings:
Recordings should be deleted once they are no longer needed for their educational purpose. Your Zoom administrator can set "automatic deletion" settings for all recordings after a certain number of days. Some units have established 100 days as the automatic deletion period, with a reminder of 7 days before the automatic deletion and a 30-day safety valve for instructors who forget after the 100 days and want to retrieve their lectures.

Protection of faculty Intellectual Property (IP) rights:
Students should be advised that lectures must not be shared with anyone outside the classroom. Inappropriate sharing may be subject to discipline pursuant to the University's student misconduct policies. For more information on protecting your IP rights, see the following guidance on protecting an instructor's IP rights.

Asynchronous alternatives to recording your course:
If you wish to avoid video recording your course, here are a few alternatives adopted by some faculty members to consider:

- Allow students the flexibility to attend a different discussion section if they cannot attend their assigned discussion on a particular day (if discussions will not be recorded).
- Provide students the option for an additional written assignment on a topic connected to the class discussion that they missed (if discussions will not be recorded).
- If an instructor does not want to video record lectures, then audio recording may also be helpful for students as it can be less invasive of privacy in that names and faces are not recorded.

9. What type of privacy laws and UC policies apply to my Zoom sessions?

Zoom classroom recordings are generally protected as Family Education Rights and Privacy Act (FERPA) records because student PII or Personal Identifiable Information (name, image, etc.) is present in the recording. The Department of Education issued COVID-specific FERPA guidance, advising that the FERPA Health & Safety Emergency Exception may be used to respond to COVID-19 pandemic safety needs. The Department of Education has also reissued Remote Learning Guidance. Zoom claims compliance with FERPA guidelines. For more information, see Zoom's FERPA Compliance Guide.

Zoom classroom recordings are subject to the UC's Electronic Communications Policy (ECP). In terms of UC-specific policies, your Zoom administrator will have access to all cloud recordings associated with your account, however, they must follow the UC Davis Policy and Procedure Manual Section 310-24, Electronic Communications—Privacy and Access to access those recordings and the UC ECP. This process requires requesting consent from the holder of that recording (you, the faculty member); or, requesting approval from the campus privacy officer and appropriate campus leadership, if the holder declines to give consent.

10. Who should I contact for help about this FAQ?

If you are aware of other Zoom privacy issues, contact the UC Davis Privacy Office at privacy@ucdavis.edu.

If you have general questions on how to use Zoom or how to activate Zoom features, contact your Unit IT Administrator. The list of contacts by College/School/Department is available here.
If you are a UC Davis Health student, faculty, or staff member, please visit this website for Zoom information.

Past Zoom privacy issues resolved by Zoom are available here.

The Zoom section of the Keep Teaching website should be your first stop.

The IT Knowledge Base websites also have resources and helpful articles:

- Zoom guide for faculty
- Zoom guide for staff
- Zoom guide for students

The summary of the changes made to the FAQs on Zoom, Privacy, and Security at UC Davis that were made on a bi-weekly basis through June 2020 are available here.

11. What about general privacy and remote teaching concerns (not just limited to the Zoom platform)? What if I would like to recommend a change to these FAQs?

This resource is focused on specific tips for Zoom classrooms. However, if sufficient faculty interest is expressed on general privacy considerations for faculty in remote teaching, the Privacy Office can develop such a resource. Please email privacy@ucdavis.edu to express your interest, provide suggestions, or if you would be willing to serve on a faculty commenter group supporting development of such a resource.

We welcome feedback on these FAQs. If you wish to recommend a change or additional guidance, feel free to email privacy@ucdavis.edu.