Guidance on Protecting Privacy and Data
During Remote Working and Teaching Using Zoom
while COVID-19 Modifications are in Effect

A. Purpose and Principles

Zoom is the primary approved remote software tool for remote live and recorded academic sessions and meetings for the campus. Zoom, when used in conjunction with the campus CCLE learning management system, , addresses privacy, security, and accessibility for people with disabilities.[1] This document provides basic guidance on how to protect privacy and data while addressing accessibility using Zoom and CCLE during remote working and teaching. Click on the hyperlinks throughout this document for quick access to important use instructions.

For more information on remote working and teaching:

- See Planning for Academic Continuity
- And for tools see Approved Remote Software Tools for campus-wide use in instruction.

The University protects the privacy of faculty, students and staff while working or participating in educational programs. Use of remote delivery software and technologies heightens the criticality of privacy and the need to use the least invasive means of engaging in these alternative methods of conducting our activities. Existing law and policy that address privacy remain in effect.[2]

All faculty, staff and students must follow these principles:

1. Video or audio recording of a lecture is permitted but only with advance notice and opportunity to opt out of video/audio participation. This requires that you download and install the native Zoom app for your computer.
    a. Where recording is permitted, it is permitted only by the host (typically instructor or meeting chair). Students in a class and/or meeting participants and any student-hosted meetings are prohibited from recording of any kind. Accommodations for students with special needs will occur through instructor recording.
2. Video or audio recording (including taping, recording, photographing, screen capture and other methods of capture) for purposes other than instruction is

[1] The guidance in this document applies to any teleconferencing service, whether used in instruction or for administrative meetings. For specific instructions on other products, please contact your IT Director.

[2] Including the policies governing student record privacy under FERPA, privacy protections afforded by the UCOP Electronic Communications Policy, the Student Conduct Code and the applicable personnel policies.

prohibited absent a strong rationale and only if the host provides advance notice and opportunity to opt out of video/audio participation.

3. During video conferencing, there is a chat function that permits participants to ask questions and engage in dialogue with the class or meeting proceeding. Recording, including photographing, screen capture, or other copying methods, of chat exchanges is prohibited except by the instructor or meeting chair when advance notice is provided.[3]

4. Online advising can occur via chat, audio, or video conferencing using Zoom or other approved software tools, or by phone. Sessions should not be recorded; rather, the advisor should log notes in the customary fashion.

B. Tips for Privacy Protections for Synchronistic Videoconferencing

1. Participants can use Zoom's virtual background feature, when available, if they do not want to have their surroundings visible.

    - To use a Virtual Background click the up arrow by the Zoom video icon and click on Choose Virtual Background.
    - Select only appropriate virtual backgrounds.
    - Be mindful of others in your remote location who may not wish to be visible or recorded in the background.
    - Ensure sensitive conversations cannot be overheard or work observed by unauthorized persons in the alternate work location.

2. Consider whether only the host needs to be visible in order to minimize bandwidth usage, and instruct participants not to enable their video if not needed. A single video stream can ease Internet bandwidth for all participants. If video of all participants is preferred, all participants should conduct themselves in the same manner as they would in an in-person setting.

    - Participants should be properly attired, should not gesture inappropriately, should not move from room to room, use the restroom, or engage in other distracting activities while still engaged in the video session.

3. Zoom default settings for the campus are set to limit screen sharing to the host. . Before screen sharing, close all applications, emails and documents that you will

---

[3] For students, the UCLA Student Conduct Code 102.28 Expectations of Privacy applies and specifically prohibits recording without the consent of all recorded parties and prohibits taking photographs where there is a reasonable expectation of privacy. In remote teaching, advising, chatting, and other engagement in course activities remotely there is a reasonable expectation that photographing, screen capture, or other copying methods or recordings will not occur without express permission from all participants. A violation subjects a student to the disciplinary process.

Section 102.23 regarding unauthorized use or sale of University Materials also applies and prohibits the distribution or sale of academic materials and course presentations.

not use in that session. The host can also allow screen sharing by participants, options are available by clicking on the up arrow by the Share Screen icon. If the host determines that screen sharing by participants is needed, the host should remind participants not to share other sensitive information during the meeting inadvertently.

4. Protect your classes and meetings delivered remotely from having unauthorized individuals join. ("Zoom bombing" is the practice of uninvited individuals entering a video call.)

    - Videoconferencing hosts should monitor participants on teleconference calls to reduce the chance of unauthorized persons on the calls.
    - Use a unique meeting ID for each meeting or require authentication and a passcode for participants (Settings → Profile → Personal Meeting ID; Meetings → Authenticate, Password).
    - Limit reuse of access codes: if you've used the same code for many meetings, others will have access to your meetings using that same passcode.

For further privacy features and options for Zoom see "Keep the Party Crashers from Crashing your Zoom Event"

C. When Audio or Video Recording is Necessary for Videoconferencing-based Courses and Meetings

1. Give notice before recording begins and preferably with the meeting invitation, in the syllabus or other scheduling tool. Approved notification language, which provides options for opting out of being recorded:

    - This [class/meeting] is being conducted over Zoom. As the host, I will be recording this session. The recording feature for others is disabled so that no one else will be able to record this session through Zoom. No recording by other means is permitted. This session will be posted at the CCLE class website unless otherwise notified. If you have privacy concerns and do not wish to appear in the recording, do not turn on your video. If you also prefer to use a pseudonym instead of your name, please let me know what name you will be using so that I know who you are during the session. If you would like to ask a question, you may do so privately through the Zoom chat by addressing your chat question to me only (and not to "everyone"), or you may contact me by another private method. If you have questions or concerns about this, please contact me.

      Pursuant to the terms of the agreement between the vendor and UCLA, the data is used solely for this purpose and the vendor is prohibited from redisclosing this information. UCLA also does not use the data for any other purpose. Recordings will be deleted when no longer necessary.

However, the recording may become part of an administrative disciplinary record if misconduct occurs during a videoconference.

2. Zoom will automatically inform all participants that the session is being recorded. Be aware not all participants may be running the latest version of Zoom that implements this feature.
3. Recordings should be retained no longer than necessary and should only be retained on approved University devices, platforms or networks.
4. Make clear on any class website that all recording is prohibited other than by the instructor.

D. Disability Accommodations and Recording of Lectures

Go to How to Record Your Lecture in Zoom and Post it in CCLE for step-by-step instructions.

E. Online Exams and Proctoring

Requiring students to turn on their camera to be watched or recorded at home during an exam poses significant privacy concerns and should not be undertaken lightly. Instructors are encouraged to consider other options that will uphold integrity and good assessment design.

During classes, students should be encouraged to use the virtual background feature of Zoom if they do not want their surroundings to be visible. However, the point of proctoring is to be able to assure that students are completing their exams independently and without assistance, so students are encouraged to take their exam in a room that has no one else present.

Several proctoring services use machine learning, AI, eye-tracking, key-logging, and other technologies to detect potential cheating. If instructors are using one of these services during the COVID-19 measures, they must provide explicit notice to the students before the exam including *that if cheating is suspected, the recording may become part of the student's administrative disciplinary record*. Instructors are encouraged to consider other options that are privacy-protective and still preserve academic integrity, where possible.

F. Online advising

Online advising can occur via chat, audio, or video conferencing but should be done using Zoom or other service approved by the campus, or by phone. Sessions should not be recorded; rather, the advisor should log notes in the customary fashion. The advisor should always be logged in on campus or through a VPN when advising.

Follow the guidance in Section B, above.

G. Privacy Data Protections with Zoom

Zoom's Privacy Policy and their Privacy Shield certification reflect that Zoom does not access data files not specifically authorized by the user (e.g. if you give Zoom access to your calendar then it will be able to read your calendar events only). Zoom does collect user data and utilizes cookies to store information on preferences. In the event you record a Zoom session, a file folder is created so that the recording can be saved through CCLE and made available for class use. The campus has turned off file sharing to prevent sharing of any files on your computer. As a user of Zoom if you give Zoom access to any files or programs you need to manage cookies through your browser settings in the way you do with other applications. Remember that UCLA policy and UC Security Standards do apply to any computer you use for your Zoom session. The relevant policies and standards are listed below.

- Policy 401 Minimum Security Controls
- Policy 404 Encryption of Electronically Stored Personal Information
- Policy 420 Breaches of Computerized Personal Information
- UCOP Minimum Security Standard