Privacy Considerations for Video Conferencing

Guidance on Protecting Privacy and Data when using Zoom to conduct remote meetings while COVID-19 Modifications are in effect. This guidance applies to administrative and instructional meetings.

I. Purpose and Principles

Zoom is one of the primary approved software tools for conducting remote/virtual meetings. This document provides basic guidance on how to protect your privacy and the privacy of others when using Zoom.

Note: For general information on best practices for working remotely, please visit the Professional & Organizational Development website and/or the Information Technology website, (Insert new AP Draft # & name with note "upon approval")

Privacy is a basis for an ethical and respectful workplace (see Board Policy (BP) 2715 / Administrative Procedure (AP) 2715 – Code of Ethics/ Standards of Practice); and privacy, together with information security, underpins the College's ability to be a good steward of the information entrusted to it by its students and employees. The College protects the privacy of faculty, students, and staff while working or participating in educational programs and other college business. 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 when we work remotely.

College security policies and procedures apply to any computer you use for your Zoom session. See BP 3721 / AP 3721 – Information Security for more specific information regarding the College's information security policies and procedures.

II. Technical Tips and Privacy Protections for Video Conferencing

1. Visibility of Remote Work Locations: Participants should use Zoom's virtual background feature, when available, if they do not want to have their surroundings visible. Managers should avoid requiring staff to use Zoom meeting settings that leave staff living areas visible.
    A. To set up a Virtual Background in Zoom click the up arrow by the Zoom video icon and click on "Choose Virtual Background".
    B. Select only appropriate virtual backgrounds.
    C. Be mindful of others in your remote location who may not wish to be visible or recorded in the background.
    D. Also, consider if all participants need to be visible, limiting the meeting to a single video stream can ease bandwidth concerns for participants.
    E. Ensure sensitive conversations cannot be overheard or work observed by unauthorized persons.

2. Screen Sharing Privacy

   A. Protecting Confidential Data on Your Device from Being Viewed: Avoid sharing confidential information that is visible on your other screens. Before screen sharing, close all applications, emails and documents that you will not use in that session.

   B. Managing Whose Screen is Visible: The host can control screen sharing by participants. Options are available by clicking on the up arrow by the Share Screen icon. The host can select the "host only" setting to prevent others from sharing their screens. If the host determines that screen sharing by participants is needed, sharing by "one participant at a time" should be selected. The host should remind participants not to share other sensitive information during the meeting inadvertently.

3. Managing Participants: Some basic tips for limited preventing unwanted attendees or Zoom Bombing are listed below:

   A. Don't post meeting IDs in public forums. Use unique meeting ID for large Zoom calls.

   B. Don't reuse meeting access codes. You can generate a new access code for each meeting.

   C. Monitor participant list for unwanted attendees

   D. Using Zoom settings for meeting participants, the meeting host can:

      i. Limit attendance to participants who are signed in to the meeting using the email listed in the meeting invited

      ii. Set up a Waiting Room Function

      iii. Password protect meeting access

      iv. Lock meetings. once they start

      v. Mute participants who are not presenting

      vi. Remove unwanted participants

      vii. Disable private chat

III. Recording of Zoom Meetings and Chats

Recording of Meetings – Notice/Consent: Do I need to obtain meeting attendee permission to capture their video and save sessions? (See AP 3710 – Filming**, Recording,** and Photography [currently under revision])

Yes. Some US states (including California) are "two party" or "all party" consent states, which generally require the permission of both or all parties involved in a recording. While attendees participating remotely may be coming from a variety of states (or countries), we must assume the "all party" consent rule applies.

Meeting hosts should always inform attendees at the start of the meeting or in advance of the meeting if they are going to record a meeting. Zoom automatically notifies attendees present at the start of a meeting if the meeting is being recorded. However, meeting hosts should also verbally notify attendees that a meeting will be recorded. Meeting hosts may also choose to explicitly require

consent to be recorded via Zoom. Attendees who do not consent will be denied access to the meeting, so we suggest its use only after you have communicated with your attendees, given them a chance to express any concerns, and determined an alternative for individuals who have not consented.

We recommend that you inform meeting attendees, prior to a recorded meeting, how you intend to record, use, and share video. You may also consider giving attendees options to participate without having their image or voice recorded, such as allowing them to attend with no video or audio, and the option to pose questions only in the text chat window. Because you can start and stop recordings in Zoom at any time, you can choose to include unrecorded time throughout your Zoom session, giving attendees an opportunity to discuss topics or ask questions that they do not wish to have recorded.

As a general rule, staff meetings should not be recorded absent an articulated business purpose (including as a reasonable accommodation) that requires recording of the meeting. Generally, you should not record a meeting if the same meeting would not be recorded if it occurred in person.

If a staff meeting is going to be recorded, hosts should inform attendees that the meeting will be recorded in advance of the meeting and also offer attendees the opportunity to opt out of the meeting or to mute their audio and video if they object to the recording of their image or voice. Please consider whether it is necessary to record the meeting. Bear in mind that the recording becomes a College record that must be stored and retained appropriately and may be subject to disclosure upon request (e.g., in response to a request under the California Public Records Act or California's Information Practices Act). If you believe it is necessary to record a meeting, but one or more participants object to the recording, please consult Human Resources.

IV. Disability Accommodations

For guidance regarding accessibility and Zoom, see the Accessibility Resource Centers for Students website or the Zoom Accessibility Considerations website. If you have specific questions regarding employee disability accommodations in connection with use of Zoom, please consult Human Resources at HRAccommodations@mtsac.edu or (909-274-4225).

V. Privacy Data Protections with Zoom

Zoom's Privacy Policy states:

We do not sell your personal data. Whether you are a business or a school or an individual user, we do not sell your data.

- Your meetings are yours. We do not monitor them or even store them after your meeting is done unless we are requested to record and store them by the meeting host. We alert participants via both audio and video when they join meetings if the host is recording a meeting, and participants have the option to leave the meeting.
- When the meeting is recorded, it is, at the host's choice, stored either locally on the host's machine or in our Zoom cloud. We have robust and validated access controls to prevent unauthorized access to meeting recordings saved to the Zoom cloud.
- Zoom collects only the user data that is required to provide you Zoom services. This includes technical and operational support and service improvement. For example, we collect information

such as a user's IP address and OS and device details to deliver the best possible Zoom experience to you regardless of how and from where you join.

- We do not use data we obtain from your use of our services, including your meetings, for any advertising. We do use data we obtain from you when you visit our marketing websites, such as zoom.us and zoom.com. You have control over your own cookie settings when visiting our marketing websites.
- We are particularly focused on protecting the privacy of K-12 users. Both Zoom's Privacy Policy (attached) and Zoom's K-12 Schools & Districts Privacy Policy are designed to reflect our compliance with the requirements of the Children's Online Privacy Protection Act (COPPA), the Federal Education Rights and Privacy Act (FERPA), the California Consumer Privacy Act (CCPA), and other applicable laws

Zooms use of Cookies:

When you log in to your Zoom account, Zoom will ask you to accept its use of "cookies".

For the most part, Zoom utilizes "cookies" that collect information about you, such as your log-in details, to enhance the functionality of its site. However, in addition to the cookies that Zoom uses to help with the functionality of its services and user experience, it also uses "advertising cookies". Advertising cookies are used by advertising companies to serve ads that are relevant to your interests.

We recommend that you "opt out" of Zoom's use of such advertising cookies, which collect information about you and your use of Zoom's site for advertising purposes. To opt out of advertising cookies, click on the "more info" option when you sign in to your Zoom account and are prompted to accept Zoom's cookies. When you click on "more info", you can then click on "cookie settings", which will take you to a menu that allows you to select which cookies you permit Zoom to use: Required Cookies/CCPA Opt Out; Functional Cookies; and Advertising Cookies. You can opt out of Advertising cookies by unselecting that option.

Despite these protections, users should use common sense and avoid sharing more information when necessary when using Zoom, especially when discussing confidential matters.

Additionally, 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 the College's AP 3710 – Filming**, Recording,** and Photography (currently under revision), and BP 3721 / AP 3721 – Information Security apply to any computer you use for your Zoom session.