Zoom Precautions for meetings and classes 4.20.20

Maintaining privacy for your students and yourself is important as we embark on this new journey in education. In addition, wherever possible, we want to prevent our students from being harassed online. If you follow the directions below, you are much less likely to have issues within your Zoom meetings.

General precautions for everyone

1. Ensure that the password you use for ConferZoom is unique, and not a password that you use for multiple other services. This is good advice for anything that requires a password in case your information is compromised with a specific application. Change this in your profile when you log into ConferZoom.org. The image below is from the bottom of the Profile page (the page where you are directed after you login.)

2. Do not post meeting or lecture links in a public forum. Send it only to the specific people invited to the meeting.
3. Ask your students not to share the meeting links with others.
4. Use your settings wisely. The important settings that will protect your Zoom meeting from interference are listed below. We encourage you make these adjustments in your settings.
5. Don’t click on links in the Zoom chat from anyone you don’t know, and encourage your students to do the same. If at all possible, don’t send links through chat at all. Send them to your students in an email beforehand.
6. Warn your students that anything they post in private chat becomes a part of the saved chat transcript that the meeting host receives at the end of the meeting.

Enable Waiting Room- of all the things you can do to protect your meeting, this might be the best step in ensuring the safety of you and your students.

Quick set up: Find your host tools from within the Zoom meeting you are hosting.

My arrow is pointed to the security settings. Once you click on that, as host, you will see the option to Enable waiting room. Make sure there is a check next to that. This works very well if you know the names of those who should be in your meeting. When someone shows up for your meeting, they won’t go straight into your meeting. They will get a message that they are in your waiting room, and you will see something that looks like this:
When I see a name I don't recognize or a number like above, I can send out a Message, as you see at the top of this image. The student cannot respond back, but you can give them a direction, such as “Rename Yourself” so you can recognize them. If the student should be in your class click admit, which will show up next to the name if you move your cursor. No one can get into your session unless you admit them, if you enable the waiting room.

Meeting host settings

Use these settings to be sure you retain control of a meeting. When you go into settings from ConferZoom.org, these options will appear.

1. Zoom recommends for your and your participants safety that you allow Zoom to generate a meeting ID for scheduled meetings instead of using your personal meeting ID. Change that setting here.

2. You can also require a password to get into your meetings. No one will be allowed in who does not have a password. For this to be effective, you need to ask your participants not to share this information.
3. One feature that has been abused previously is the virtual background. This can be a fun way for participants to express themselves, but virtual backgrounds can be used to harass participants. Turn this feature off if you can’t control other aspects of your meeting, such as enabling a waiting room. You will find this feature under the **In Meeting Advanced** tools.

![Virtual background](image) - Allow users to replace their background with any selected image. Choose or upload an image in the Zoom Desktop application settings.

4. While chat can be handy while you lecture, you can avoid issues that come up in chat by turning this feature off. Determine what works best for your class and warn students that the host gets a copy of all chat, private or not when the meeting is over if you choose to keep this feature enabled.

![Chat](image) - Allow meeting participants to send a message visible to all participants
- Prevent participants from saving chat

![Private chat](image) - Allow meeting participants to send a private 1:1 message to another participant.

![Auto saving chats](image) - Automatically save all in-meeting chats so that hosts do not need to manually save the text of the chat after the meeting starts.
5. File transfers can be used to send documents to your students but you can turn this feature off if you want to avoid any security issues that might come from someone sending files through chat.

   **File transfer**
   Hosts and participants can send files through the in-meeting chat.  
   - [ ] Only allow specified file types

6. Eliminating the ability for participants to share their screen will reduce risk of students or others causing a disturbance in class.

   **Screen sharing**
   Allow host and participants to share their screen or content during meetings
   
   **Who can share?**
   - [ ] Host Only
   - [ ] All Participants

   **Who can start sharing when someone else is sharing?**
   - [ ] Host Only
   - [ ] All Participants

7. Allowing participants to annotate the whiteboard or other documents also presents the possibility of students or others causing a disturbance. Use these tools if you need them, but knowing where to turn off the ability for others to use them can be helpful if you have problems.

   **Annotation**
   Allow participants to use annotation tools to add information to shared screens

   **Whiteboard**
   Allow participants to share whiteboard during a meeting
   - [ ] Auto Save whiteboard content when sharing is stopped

8. Allow participants to rejoin- this should be turned off in almost every instance. If you remove a participant there is probably not a good reason to allow them to rejoin.
9. If someone causes a disturbance in your class, you can mute all participants and then take away the ability for participants to unmute themselves. This is a two-step process. Click on Manage Participants and this screen will pop up. You can see the option to mute all directly above. Then click more, and turn off the option that allows participants to unmute themselves.

10. Lock meeting. A more extreme measure is also seen from the Manage Participants screen above. If you have had issues with participants causing trouble, or you just want to ensure that no one comes into your meeting that you don’t want there, go to the more tab above in the Manage Participants window and select lock meeting. No one will be able to enter the meeting from that point on.
Zoom recently added a new security feature in Host Tools. Click on the security icon to access all of the following directly:

- Lock Room
- Enable Waiting room (as seen at the beginning of this document)
- Manage participant ability to: Share screen, chat, and Rename themselves

**** FERPA requirements. Please review this information from @One Education regarding our requirements in terms of our students’ privacy when using Zoom.

https://onlinenetworkofeducators.org/2020/04/03/guidance-for-recording-zoom/