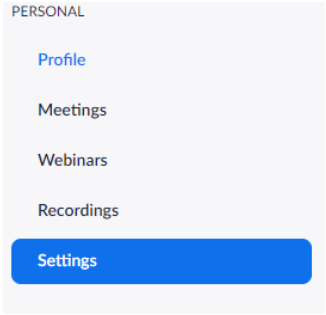
# Online Zoom Meeting Hosting Guidelines

*Purpose: to protect everyone's anonymity, ensure smooth running of meetings, protect data & privacy.*

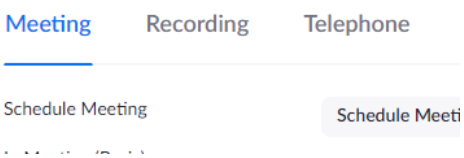
## 1. Zoom settings

*(needs to be done only once per account prior to setting up a meeting, not before every meeting)*

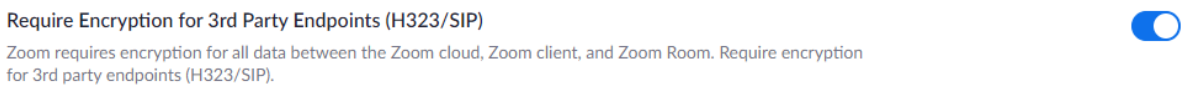
a. On the Zoom website, log in with the account you use to host meetings
b. Navigate to: Settings



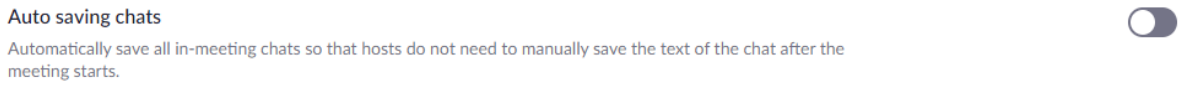

c. In the Zoom Settings section, under the Meetings subtab enable/disable the following options:




- **Enable: Require Encryption for Third Party Endpoints** *(privacy protection)*

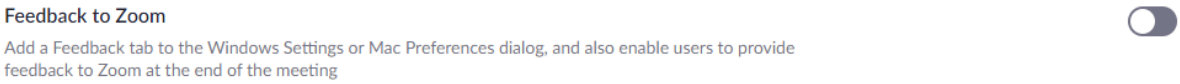


- **Disable: Auto saving chats** *(anonymity and privacy protection)*

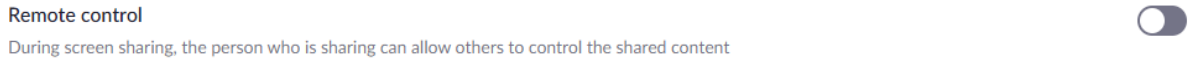



- **Disable: File transfer** *(protect against potential copyright infringement or sharing of indecent content)*

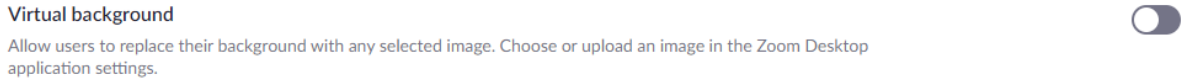

- **Disable: Feedback to Zoom** *(privacy protection)*



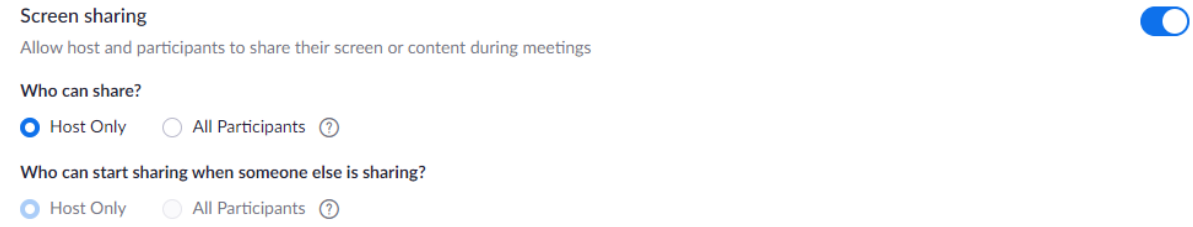

- **Disable: remote control** *(anonymity and privacy protection)*



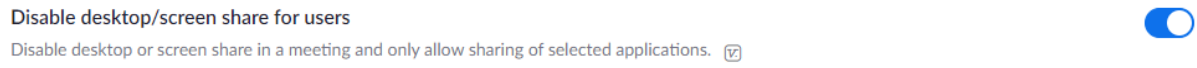

- **Disable: Virtual Background**



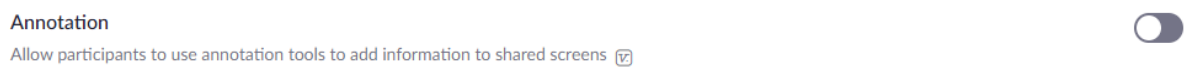

- **Enable: Screen Share for Host only** *(disruption, data protection)*




- **Enable: Disable desktop/screen share for users**

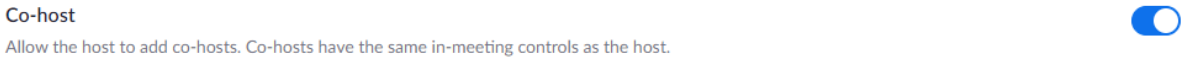



- **Disable: Annotation**

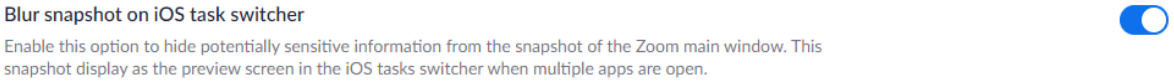



- **Disable: Whiteboard**

- **Enable: Co-Host feature** *(during meeting host can assign co-host)*

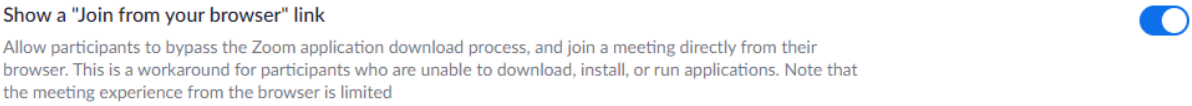



- **Enable: Blur snapshot on iOS task switcher** *(anonymity and privacy protection)*

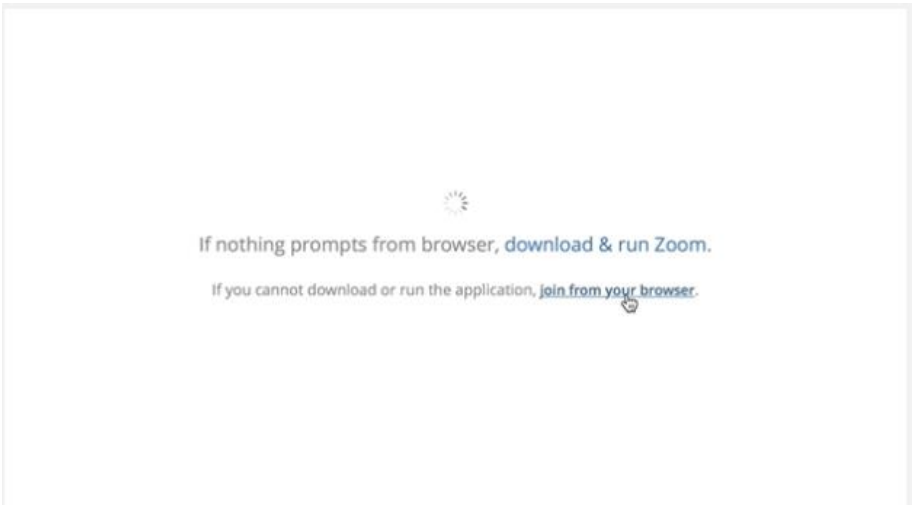



- **Enable: Show a "Join from browser" link**

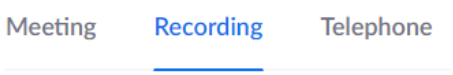
  *For individuals who cannot install any software on their work computer i.e. commission workers, meetings via this option may work unless further preventative measures are installed on the computer*




  When a participant clicks the meeting URL, instead of clicking download & run Zoom they should click **join from your browser.**

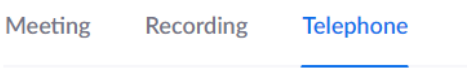



d. In the Zoom Settings section, under the Recordings subtab enable/disable the following options:

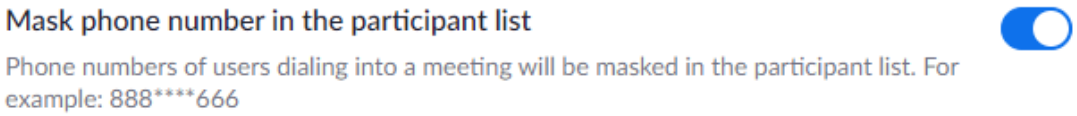


- **Disable: Local recording** *(anonymity and privacy protection)*
- **Disable: Cloud recording** *(anonymity and privacy protection)*
- **Disable: Automatic recording** *(anonymity and privacy protection)*


e. In the Zoom Settings section, under the Telephone subtab enable/disable the following options:




- **Enable: Mask phone number in the participant list** *(anonymity and privacy protection)*



# 2. Meeting Setup

- Topic
    - Choose a meeting name that preferably does not include AA. This is for added anonymity if attending meetings in public spaces
- Disable: Registration
- Disable: Require Password
- Video:
    - Enable Video OFF for Host and Participants (it means video is switched off when host or participant joins the meeting but can be turned on after that)
- Audio:
    - Enable: Both
        - Click Edit to update the country list
- Meeting Options:
    - Disable: Enable join before host *(This prevents people from joining the group before a host logs in. See "Enable Waiting Room")*
    - Enable: Mute participants upon entry
    - Enable: Enable Waiting Room *(helps you see who is trying to enter your meeting by placing them in a separate area at the top of your participants list until you let them into the main meeting. It also prevents you from getting flooded with disruptive people because it gives you a pre-emptive chance to see who is trying to enter your meeting. Wouldn't it be nice to be able to stop someone from naming themselves, say, "GateKrasherFU" or keep known bad actors from even entering your meeting at all in the first place? Waiting Room let's you do just that. You're not going to catch everybody, of course but even that occasional bad actor that does get in won't be able to unmute themselves, upload files, take over screen share or chat anyway. And who knows, maybe they might even get sober? Of course, nothing prevents them from raising their hand and once called upon to start their obscene gibberish, but at least it's only one person, very easy to ban and not let back in for the rest of the meeting. Just like what happens at real meetings sometimes.)*
    - Disable: Only authenticated users can join

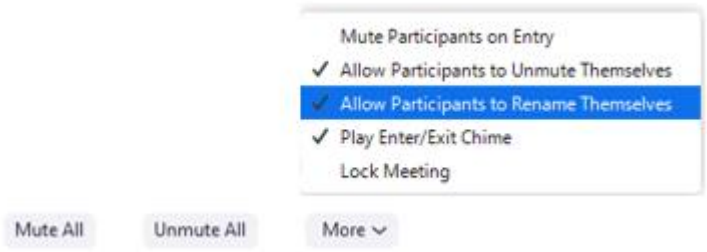
# 3. Suggested practices during a meeting

- **Ask someone to volunteer for and make them a Co-Host**

  They can keep an eye on the participant box as well and take measures against meeting trolls and attacks. Two people acting calmly and fast is better than one.

- **Disable: User Rename** *(disruption)*

  A bad actor can post something nasty in your chat and then quickly rename themselves. Their posted chat will retain the old name but they will already be cloaked with their new name as you try to find them and ban them.




- **Video participation and names** *(anonymity)*

  Some may not have their video on. Others may show their full name in the participant box unintentionally. Using Video is not compulsory and participants are free to use whatever name they please. We suggest participants use video for an immersive experience for everyone.

  We suggest participants type their first name into the system when they join. It can be checked one their own screen and in the participant box.

  We suggest the host say and/or writes via chat message before meeting starts :

  *"Using video during the meeting is your personal choice. We only ask that you use your first name so it shows in the participant box, check your screen what your current username is and verify it in the participant box. If it's anything but your first name like 'iphone' 'samsung' … whatever, contact the host either verbally or via chat box to let them know what your first name is so they can rename you. The rename feature has been disabled for participants for security reasons. Before your next meeting we encourage you to learn how to name yourself ahead of joining."*

- **Participation calls via Landline**

  *may not be able to mute/unmute themselves either because their (landline) phone doesn't support it or they may be visually impaired. It is suggested hosts ask the*

*caller whether they can unmute themselves. If not they stay unmuted if at all possible throughout the entire meeting or suggest to keep them muted until invited by the host to share.*

# 4. What to do if a meeting is attacked

Expect explicit, obscene porn, lewd images, foul language and verbal abuse (often directed at the lead/chairperson to invoke chaos). First and foremost, remain calm, having expected to experience this. Shock their primary goal. If you are calm, you can act quickly and decisively instead of react.

Having already blocked their ability to video-share, which is their primary weapon, the only thing that intruders can do now is post deplorable images, show live video from their device, and/or verbally abuse, which they seem to like to do in gangs of many in order to rapidly overcome a meeting.

1. If this happens (you will have no doubts), immediately click the “Mute All” button (turns blue)

2. Quickly uncheck the option “Allow attendees to unmute themselves” nearby, under ‘More’ (just next to the Mute All/Unmute All buttons. This essentially gives Zoom-bombers no reason to stay on at this point, and they likely will start dropping once they see that you know how to take away their ability to disrupt a meeting. Under normal meeting circumstances, you want members to be able to mute and unmute themselves in order to engage more naturally with the group as we would in face-to-face meetings, so blocking attendees from unmuting themselves should be a temporary action until the intruders have left.

3. Feel free at any time, unmuting yourself and your co-hosts, to inform the audience what you’re doing (while attendees remain force-muted, things tend to get awkward), putting a temporary hold on the meeting while the problem is being addressed. Let them know the meeting will restart shortly.

4. During this hold period, have your co-host(s) along with you, click on “Participants”, go through and “Remove” all the obviously bad actors. You can also distinguish most of them from the names or images they post for themselves. Sometimes they will have video on, being their only chance left to show a shock video, with the camera pointing somewhere random like a ceiling fan. If you are unsure and don’t want to drop someone who may be an actual AA member, unmute them and request that they identify themselves. Trolls either won’t identify or they will say something making it obvious they are a troll, or they’ll just stay silent or drop altogether.

5. Under “More” settings, select the “Lock Meeting” option at a certain point early on, for example, after the readings. This prevents anyone from joining after a period of time of your choosing.

6. Once you've experienced this a few times, it will be easier and troll groups will find your meeting "no fun" and will move on. If we get enough of our groups shutting them down, they will stop having any reason to Zoom-bomb our AA meetings.

7. Password-protected meetings are also an option - but newcomers, having no face-to-face meeting options today, will have no way to get invited to a password-protected meeting. So take That route only if you intend to have a closed meeting by invitation only, keeping the traditions in mind.