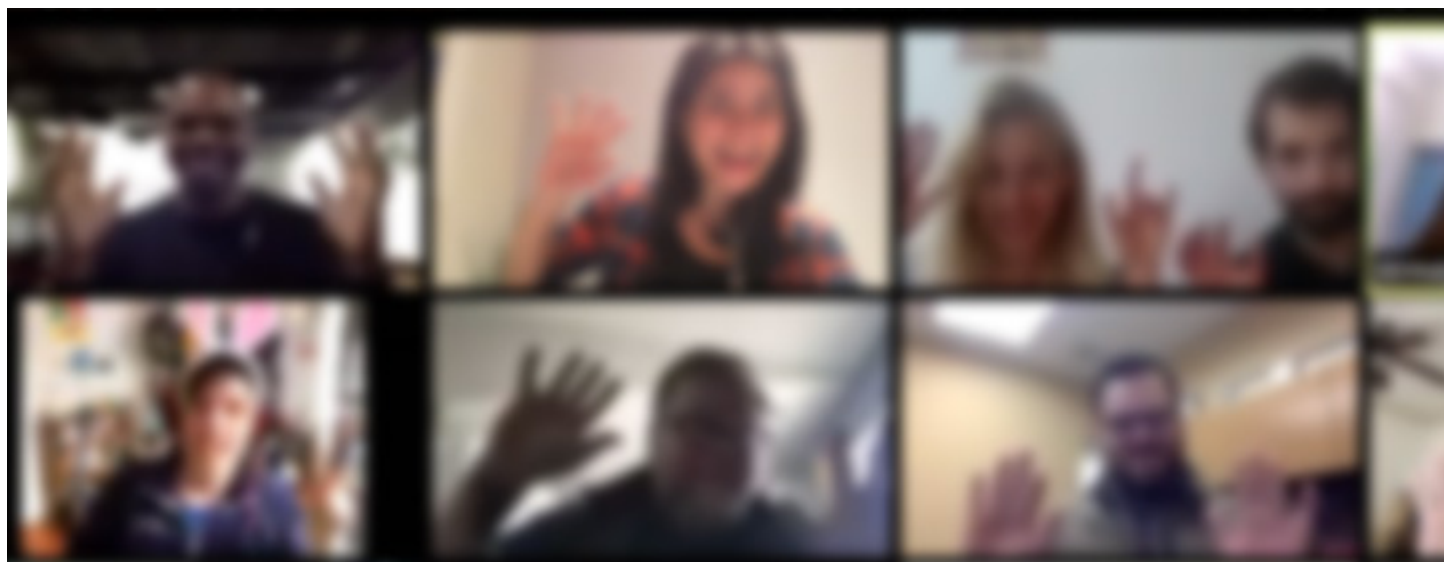# Online AA Zoom Meeting Hosting Guidelines

These online AA Zoom meeting guidelines are based on guidance released by GSO. These are intended to help those who are hosting online zoom meetings and to help protect everyone's privacy and anonymity.

1. Zoom settings

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

On the Zoom website, log in with the account you use to host meetings. Then navigate to: Settings.

PERSONAL

Profile

Meetings

Webinars

Recordings
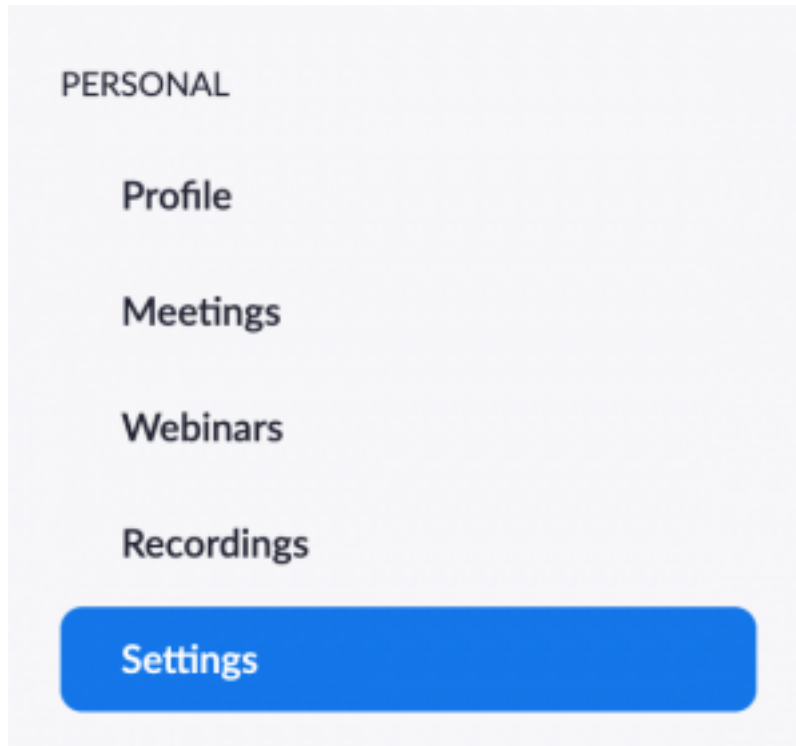
Settings

In the Zoom Settings section, under the Meeting subheading, do the following.

Meeting   Recording   Telephone

Schedule Meeting

In Meeting (Basic)

In Meeting (Advanced)

Email Notification

Other

Schedule Meeting

Host video
Start meetings with host video on

Participants video
Start meetings with participant video on. Part
change this during the meeting.

- Enable 'Require Encryption for 3rd Party Endpoints'.

In Meeting (Basic)

Require Encryption for 3rd Party Endpoints (H32

Zoom requires encryption for all data between the Zoom
Zoom client, and Zoom Room. Require encryption for 3rd
endpoints (H323/SIP).

- Disable 'Auto saving chats'.

Auto saving chats

Automatically save all in-meeting chats so that hosts d
need to manually save the text of the chat after the me
starts.

- Disable 'File transfer'.

File transfer

Hosts and participants can send files through the in-m
chat. [V.]

- Disable 'Feedback to Zoom'.

Feedback to Zoom

Add a Feedback tab to the Windows Settings or Mac Preferences dialog, and also enable users to provide fe to Zoom at the end of the meeting

- Disable 'Remote control'.

Remote control

During screen sharing, the person who is sharing can others to control the shared content

- Disable 'Virtual background'.

Virtual background

Allow users to replace their background with any sele image. Choose or upload an image in the Zoom Deskt application settings.

- Enable 'Screen sharing' for host only and click save.

Screen sharing

Allow host and participants to share their screen or con
during meetings

Who can share?

◉ Host Only   ○ All Participants

Who can start sharing when someone else is sharing?

○ Host Only   ○ All Participants

Save   Cancel

- Enable 'Disable desktop/screen share for users'.

Disable desktop/screen share for users

Disable desktop or screen share in a meeting and only
sharing of selected applications. [v.]

- Disable 'Annotation'.

Annotation

Allow participants to use annotation tools to add infor
shared screens v.

- Disable 'Whiteboard'.

Whiteboard

Allow participants to share whiteboard during a meeti

- Enable 'Co-host'.
- 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'.

Show a "Join from your browser" link

Allow participants to bypass the Zoom application dov
process, and join a meeting directly from their browse
workaround for participants who are unable to downlo
install, or run applications. Note that the meeting expe
from the browser is limited

- Enable 'Blur snapshot on iOS task switcher'.

Blur snapshot on iOS task switcher

Enable this option to hide potentially sensitive informa
the snapshot of the Zoom main window. This snapsho
as the preview screen in the iOS tasks switcher when
apps are open.

Now go back to the top of the settings screen and select the 'Recording' tab.

- Disable 'Local recording'
- Disable 'Cloud recording'
- Disable 'Automatic recording'

Meeting   **Recording**   Telephone

Recording

Local recording
Allow hosts and participants to record the meeting to a local file

Automatic recording
Record meetings automatically as they start

Recording disclaimer
Show a customizable disclaimer to participants before a recording starts ⊡

Multiple audio notifications of recorded meeting
Play notification messages to participants who join the meeting audio. These messa
the recording starts or restarts, informing participants that the meeting is being rec
participants join the audio from telephone, even if this option is disabled, users will
notification message per meeting.

Again, at the top of the settings screen, select the 'Telephone'
tab.
- Enable 'Mask phone number in the participant list'.

Show international numbers link on the invitation email

Show the link for Zoom International Dial-in Numbers on email invitations

Toll Call

Include the selected numbers in the Zoom client and the email invitation via the inter
Participants can dial into meeting with the numbers

Mask phone number in the participant list

Phone numbers of users dialing into a meeting will be masked in the participant list. F
888****666

Global Dial-in Countries/Regions

Click the Edit icon to choose countries/regions that frequently have participants who
meetings. The dial-in phone numbers of these locations appear in the email invitation
participants dialing in from those locations.

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'.
  This means that video is switched off when the host or a participant joins the meeting but can be switched 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.
- Enable 'Mute participants upon entry'.
- Enable 'Enable Waiting Room'.
  This 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. Waiting Room lets you do that.
- Disable 'Only authenticated users can join'.
-

3. Suggested meeting practices

- 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'.

  A disruptive person can post something inappropriate 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 to remove 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 on 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 such as 'iphone' 'samsung' ..., 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 telephone

  Telephone participants 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 disrupted

- You may experience explicit, obscene or lewd images, foul language and verbal abuse (often directed at the lead/chairperson). First and foremost, remain calm. If you are calm, you can act quickly and decisively.
Having already blocked the ability to video-share (above), the only thing that intruders can do now is post inappropriate images, show live video from their device, and/or verbally abuse. This may happen from several people all at once.
- If this happens, immediately click the 'Mute All' button (turns blue).
- Quickly uncheck the option 'Allow attendees to unmute themselves' nearby, under 'More' (just next to the Mute All/Unmute All buttons). This essentially gives the intruder(s) no reason to stay and they will very probably leave. 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.
- Feel free at any time to unmute yourself and your co-hosts, to inform the audience what you're doing (while attendees remain force-muted, things tend to get awkward). Let them know the meeting will restart shortly.
- During this hold period, have your co-host(s) along with you, click on 'Participants', go through and remove the disruptive participants. You can also distinguish most of them from the names or images they post for themselves. 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 themselves or they will say something making it obvious that they are a troll.

- 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.
- Once you've experienced this a few times, it will be easier to handle and disruptors will move on.
- Password-protected meetings are also an option - but newcomers, having no face-to-face meeting options at present, will have no way to get invited to a password protected meeting. It is suggested that you take that route only if you intend to have a closed meeting by invitation only, always keeping the traditions in mind.