



Online Zoom Meeting Hosting Guidelines

April 2020



Purpose: Suggested guidance to ensure compliance of the 12 Traditions of AA when using online Zoom meetings.

The Twelve Traditions

1. Our common welfare should come first; personal recovery depends upon A.A. unity.
2. For our group purpose there is but one ultimate authority — a loving God as He may express Himself in our group conscience. Our leaders are but trusted servants; they do not govern.
3. The only requirement for A.A. membership is a desire to stop drinking.
4. Each group should be autonomous except in matters affecting other groups or A.A. as a whole.
5. Each group has but one primary purpose — to carry its message to the alcoholic who still suffers.
6. An A.A. group ought never endorse, finance, or lend the A.A. name to any related facility or outside enterprise, lest problems of money, property, and prestige divert us from our primary purpose.
7. Every A.A. group ought to be fully self-supporting, declining outside contributions.
8. Alcoholics Anonymous should remain forever non-professional, but our service centers may employ special workers.
9. A.A., as such, ought never be organized; but we may create service boards or committees directly responsible to those they serve.
10. Alcoholics Anonymous has no opinion on outside issues; hence the A.A. name ought never be drawn into public controversy.
11. Our public relations policy is based on attraction rather than promotion; we need always maintain personal anonymity at the level of press, radio, and films.
12. Anonymity is the spiritual foundation of all our traditions, ever reminding us to place principles before personalities.

In the Zoom Settings section, under the Meetings subtab, it is suggested that you enable/disable the following options:

- Enable** Require Encryption for Third Party Endpoints
 - Disable** Auto saving chats
 - Disable** File transfer
 - Disable** Feedback
 - Disable** Screen sharing
 - Disable** desktop/screen share for users
 - Disable** Remote control
 - Disable** Local recording
 - Disable** Cloud recording
 - Disable** Automatic recording
 - Disable** Local and Cloud recording features
 - Enable** Mask phone number in the participant list
 - Enable** BLUR screenshot on IOS Task Switcher
 - Disable** Only authenticated users can join meetings: Participants need to authenticate before joining the meetings.
 - Disable** Join Before Host
 - Disable** Virtual background
 - Disable** Breakout room
 - Disable** Waiting room
 - Disable** Lock meeting
- Take care when using your name or email address to log in as these may be displayed at the start of the video call*

Establishing the Meeting

Secretary to:

- ensure attendees are aware of any Group Conscience decisions regarding changes to Zoom settings of the meeting.
- remind members of the importance of anonymity (their own and others).
- reminder - no use of the chat function during sharing (except to request help from the Host or Admins). This feature can be disabled if it becomes an issue.
- welcome newcomers.
- share available methods of continuing to make Tradition 7 donations.

Host to:

- ensure attendees can use the necessary Zoom functions to engage with the meeting (Raise Hand, Unmute, Rename (first name only) etc.)
- brief attendees on the protocol to be followed if the meeting were to be 'attacked'.

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 is their primary goal. If you are calm, you can act quickly and decisively instead of reacting.
- 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.

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 intruders 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. When you can, unmute yourself/the Secretary to inform the audience what you're doing, if necessary, putting a temporary hold on the meeting while the problem is being addressed. Let them know the meeting will restart shortly if it cannot continue.

4. Under "More" settings, select the "Lock Meeting" option - this prevents anyone else from joining the meeting **while you deal with the intruders.**

5. During this hold period, click on "Participants", go through and "Remove" all the obviously bad actors. You can 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. 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.

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, unless they come in via our Telephone Service, one of the contact email addresses on our Intergroup webpage or another member.

As always, each group is autonomous. It is suggested a Group Conscience be held for settings to be agreed upon. While it is very tempting to use particular 'security' features that are available, members are reminded to consider our Primary Purpose and Twelve Traditions when deciding on the appropriateness of using such features. Groups are encouraged to have their own Zoom Licence in-line with Tradition 7, as well as to ensure security features can be accessed and utilised when needed.

Please be advised that this guidance is the **only** guidance agreed and issued from Coventry and Warwickshire Intergroup. Any updates will be sent from one of the following email addresses:

chair.cwarwick@aamail.org

secretary.cwarwick@aamail.org

ecomm.cwarwick@aamail.org

