

## ACA ZOOM SAFETY TIPS

Every group is autonomous, so how your meeting's Zoom room safety is organised is up to your group. These tips are to help you and your group gain confidence and keep your group a safe place for all.

It's ideal that Zoom hosts and co-hosts have a fairly good understanding of Zoom room security settings; where to find the settings, and how to use them effectively. It's recommended that each meeting has a host and at least one co-host to take care of the technical side of your meeting and they all know how to remove zoom bombers. Some group's refer to their Host as "Tech Host", for this document the terms Host and Co-hosts are used.

It's possible to set the security settings from the Zoom account web portal enabling automatic security for your room when you enter, but this will need to be done by the account administrator/s who will have the room's email address, safe password and permission to make changes to the account settings.

If you keep your Zoom room an open room for anyone to join at any time, an appointed host or co-host will need to 'Claim Host' before the meeting starts, and will need to have the unique Host Key Code number in order to check and set the in- room security that you require. The Host Key Code can be supplied by your Zoom account administrator/s. Operating your meetings from an open to anyone at any time setting, and not having someone to 'Claim Host' is not advised. Your room will not be secure.

Please be aware that hosting or co-hosting a meeting from an android phone or iPad is not recommended- this is because buttons are hard to access quickly and some of the zoom facilities will be limited. if you are attending a meeting via a phone or iPad you may not see what others are seeing who are on laptops.

Some groups arrange get-togethers at a convenient time separate from their regular meetings in order to learn hosting skills, go through the security settings and experiment with all the options. The more people in your group who can do hosting/co-hosting service, the better!

## SECURITY ONCE IN YOUR ZOOM ROOM

1. Ideally, the Host or a co host will be the first one/s to access and occupy the Zoom room and can do so in good time before the meeting and arrival of other participants. Once you are in the room check the following settings:

2. **'Participants'**: Click on 'Participants' at the bottom of the screen. If you need to 'Claim Host' click on Claim Host button at the bottom of the participants box and enter the host key number for the meeting. After doing this, you can change your name (ie Jane D - Host)

3. **'Enable Waiting Room'**: Click on the Security shield at the bottom of the screen and from the pop up menu click on 'Enable the Waiting Room'. NOTE: Even if you think your room settings are already enabled via the Zoom account settings portal, check them all anyway as it's feasible someone may have altered the settings.

4. **'Whiteboard'**: Click on the 'Whiteboard' icon, at the bottom of the screen and check the 'Whiteboard' setting, and set it so the host or co-hosts are the only ones who can use the 'Whiteboard'- or disable the Whiteboard altogether clicking on the toggle. If you wish, the 'Whiteboard' can be disabled via your Zoom platform account settings and the 'Whiteboard' icon will not appear on your screen. Zoom bombers have been known to commandeer the 'Whiteboard' to display imagery, so it's best to have it disabled or set the host only option.

5. **'Share Screen'**: Click on the smaller arrow to the right of the Share Screen icon at the bottom of the screen, then click on 'Advanced Sharing Options' and tick 'Host', in answer to "Who can share?". Also tick 'Host', in answer to "Who can start sharing when someone else is sharing?" This means that only a Host or Co-Host can share the screen for readings. If your Share Screen is open to anyone, it's another way for a Zoom bomber to take over the screen for their purposes.

6. **'Chat'** box: Chat can be opened by clicking either the Chat icon at the bottom of your screen, or the 3 dots above 'More' at the far right bottom of the screen. Once the Chat box is open, there are 3 small dots bottom right where you will see options. Set the chat function setting so participants can only chat with the host and co-hosts upon entering and during the meeting. Once sharing has ended, the chat options can be changed so that all participants may chat with "everyone and anyone directly". This enables the treasurer to post the 7th tradition payment link, or for anyone else who wishes to post links for ACA events or other useful ACA information. This also allows participants to share telephone numbers directly and privately with another participant if they choose.

7. **'Name changing'**: Click on the Security shield and there is a "Rename Themselves" option. Some groups uncheck the "Rename Themselves" option to prevent zoom bombers who have entered the room from changing their own name to the name of a participant who is already in the room. The zoom bomber does this to make it more difficult for the host/co host to identify who the zoom bomber is, by having 2 people with the same name. If a participant needs their name changed, they can message the host, and the host can change the participant's name, or the host can ask the participant if they would like the host to change it for the participant.

8. Your meeting is now ready to admit participants via the waiting room.

9. **Making people Co-hosts**: Once people begin to enter the room, the Host can make the allocated people Co-hosts by going to The Participant's box, placing the cursor over the person's name and clicking on the 'More' button, the drop down menu will have an option to 'Make Co-host' ( NOTE: the person screen sharing will need to be made a Co-host as well in order to screen share, it's also good practice to make the Secretary a Co-host as well so participants can send the Secretary a message if there is an issue.

10. **Camera (video) on or off**: For the meeting's safety it is suggested that participants have their camera on when entering the room and leave it on for a couple of minutes. You can check to see if a participant in the waiting room has their camera turned on or if they have it turned off - their video icon will have a red slash through it if it's off. If you choose, you can message a participant while they are in the waiting room and request they have their camera on. 'Video on' and 'Mute when participants enter the room' can be set from your Zoom account web portal settings. It is possible to pre-set a message in the 'Waiting Room' for joining participants. This can also be done via your Zoom account setting's webpage.

11. **Locking the meeting**: Consider locking the meeting once sharing has commenced, or 'Lock' at a point decided by the group. Some groups lock after 10 minutes, some lock before the "feeling check in". It's up to your group to decide. Locking is done via the security shield menu by a Host or Co-host.

12. **Late arrivals**: Some groups choose to keep late arrivals in the waiting room for a couple of minutes. Zoom bombers often arrive after the meeting has started and might be put off by being kept waiting. Once the late arrival has entered the meeting, and when it's appropriate, the secretary can ask the late arrival to introduce themselves to the meeting.

## **DEALING WITH ZOOM BOMBING**

If zoom bombed - Have a plan of action so the host and co-hosts can together take steps to pause the meeting and calmly inform everyone that there is a disruption that needs dealing with. Coordinated effort by the host and co-hosts is encouraged. For example, the host can take charge of the identification and removal and the reporting of the disruptor, while the co-host locks the meeting and mutes everyone. Basically, what you want to achieve is:

A. Identify the zoom bomber/s as quickly as possible

B. Let the other participants know there is an issue and it is being dealt with

C. If the meeting is not already locked by this point, click on the Security Shield to 'Lock' the meeting so the disruptor/s cannot re-enter after their removal

D. Click on the drop down menu on the top right of the disruptor's video, or next to their name in the participant's box to MUTE, and if necessary click immediately on REMOVE and report them via the Zoom form that will immediately appear on the host's/co-hosts screen after removal.

E. OR you can mute everyone in the meeting via the Security shield by unticking 'Unmute Themselves'- this disallows participants to share their audio.

F. 'Suspend all participants': This option is often referred to "The Nuclear Option" and it's recommended to be used only if there is an extreme incident and it's difficult to identify, isolate and remove the disruptor/s. Click on the security shield and click on '**Suspend all Participants**' option ( in red type at the bottom of the pop-up menu) NOTE: the host and co-hosts will not be suspended, and can talk to one another to establish who is causing the disruption, then REMOVE the disruptors and REPORT via the Zoom form that will appear on the screen. Hopefully you can resume the meeting without further issues. NOTE: It will take time to get all your participant's cameras/video and audio back on. You can reset the video and audio from the security shield or via the participant's box, next to each person's name.

G. Consider having a plan to re-regulate the meeting after a disruption, possibly by acknowledging there was an unfortunate disruption, followed by a moment of silence, saying The Serenity Prayer, have a feeling's check in, or offer fellowship support after the meeting.

NOTE: It is possible that a genuine participant might inadvertently be presenting as a Zoom bomber because they are not muted and their audio is picking up noises in their room. Always check that everyone who is not speaking is muted. If you are not sure about someone- place them in the waiting room and message them to explain and make a decision to allow them back in or not.

## **EXTRA TIPS ON HOW TO MINIMISE ZOOM BOMBING**

*(as recommended by ACA UK)*

1.Ensure your zoom account has applied the most recent zoom platform updates. More current zoom updates have better safety features, this is especially important if you're the host/tech host or co-host of a meeting.

2.Don't advertise your meeting login details online: Instead, either use the one click link as it's not as easy for the details to be found and shared en masse, **or take your login details o your meeting page altogether and post a message requesting meeting information/ID etc via the group's email address.** To change details and info about

your meeting use the contact form on the ACA UK Meeting webpage; <https://www.adultchildrenofalcoholics.co.uk/meetings/>

To change how your meeting is listed on the WSO website- go to 'Meetings' tab, dropdown to 'Update or verify Meeting'. You will need your WSO number. NOTE: It appears that most Zoom Bombing is done via the links on the WSO meeting listing's. Requesting that people email ahead of time for a meeting's info seems to be very effective in reducing the chances of being zoom bombed. <https://adultchildren.org/meeting/meeting-changes/>

3.Change your login details periodically: This includes your Zoom account password, and if you use it, your host key, plus your meeting ID and Password. This is all done via the zoom accounts web page portal that can be accessed by the zoom account administrator. Periodic changes are important, especially if you have shared these details with members of your meeting who no longer attend.

## **USEFUL LINKS**

### ***Zoom Learning Centre***

<https://learn-zoom.us/show-me>

### ***ACA UK Safety information page-***

<https://www.adultchildrenofalcoholics.co.uk/safeguarding/>

If you have any questions or want to voice any issues regarding the safety of an ACA meeting please contact: [safeguard@adultchildrenofalcoholics.co.uk](mailto:safeguard@adultchildrenofalcoholics.co.uk)

*This document is compiled using information shared by ACA UK members 2023*