GUIDE FOR GROUPS

Security Settings for Zoom

Zoom has attracted a lot of media attention since its usage became widespread; from social gatherings to Number 10 Downing Street. Unfortunately not all this attention has been positive with a number of people actively seeking out security flaws or Zoom Bombing calls.

However, in most cases this has been a result of how the software has been set up rather than the system itself. So to help avoid this we've collated some of the key points to ensure a more secure meeting here:

Check Your Settings

- **Use a unique ID for large or public Zoom calls** – Every call on Zoom has a Personal Meeting ID (PMI) if you keep that to a permanent one anyone with it can join your calls whether invited or not! Look for the Meeting ID options and check its set to generate automatically.
- **Password protect your Zoom meetings.** You can set a password to join your Zoom meeting. You can require a password for new meetings, instant meetings, PMI meetings or even phone participants. You can also choose not to include the password in the meeting link.
- **Don't share you meeting link of public forums or platforms –** If you're having a public event get individuals to register for the event in advance so you can email them the details separately. Once your meeting details are in the public domain anyone could join!
- **Disable 'join before host.'** The Zoom Meeting join before host option allows meeting participants, unwanted or not, to join your meeting before you, as host start the meeting. It is always best for you to join as the host before allowing others to join so that you can see who is joining. If you must use the 'join before host' option, you should assign a password to protect the meeting.
- **Use a waiting room** - One of the best ways to use Zoom for public events is to enable the waiting room feature. The waiting room is a holding area that stops your guests from joining until you're ready for them. Meeting hosts can customize Waiting Room settings for additional control, you can also personalise the message people see when they hit the waiting room so they know they're in the right place.

- **Manage screen sharing –** Always set screen sharing to 'host only'. If you forget the host can override screen sharing from a participant (see the meeting tips).
- **Disable file transfers in settings –** Again this prevents unwanted content being shared in your meetings.
- **Use mute** - You can also enable ‘mute upon entry’ in your settings to keep the clamour at bay in large meetings.

In Meetings

- **Be careful not to share your meeting ID** - If sharing a photo of the meeting make sure the meeting ID (top left corner) is hidden
- **Lock the meeting**: Think of it as shutting the door once the meeting has started! It means no new participants can join, even if they have the meeting ID and password (if you have required one). In the meeting, click Participants at the bottom of your Zoom window. In the Participant’s pop-up, click the button that says Lock meeting.
- **Remove unwanted or disruptive participants**: From that Participants menu, you can hover your mouse over a participant’s name, and several options will appear, including remove. Click that to kick someone out of the meeting. By default, an ousted guest cannot re-join. If you make a mistake you can allow a booted party to re-join. Enable this feature by going to the web portal and navigating to Settings > Meeting > In-Meeting (Basic). Toggle on the setting called; Allow removed participants to re-join.
- **Put them on hold**: You can put everyone else on hold, and the attendees’ video and audio connections will be disabled momentarily. Click on someone’s video thumbnail and select Start Attendee on Hold to activate this feature. Click Take off Hold in the Participants list when you’re ready to have them back.
- **Disable someone’s camera** - Hosts can turn off any participant's camera. If someone is being rude or inappropriate on video, or their video has some technical problem, the host can open the Participants panel and click on the video camera icon next to the person's name.
- **Mute participants**: As you probably know already you can mute / unmute individual participants or all of them at once. Hosts can block unwanted, distracting, or inappropriate noise from other participants.
- If you forget to change your **screen sharing** settings before the meeting you can do it during the call. Use the host controls at the bottom of the screen, click the arrow next to Share Screen and then Advanced Sharing Options. Under ‘Who can share?’ choose ‘Only host’ and close the window. You can also lock the screen share by default for all your meetings in your web settings.

- **Disable private chat** - If you're hosting a Zoom call and have invited strangers to join and you're concerned they could harass someone or send inappropriate private messages, you can prevent this by disabling private chat. When you disable private chat, it doesn't affect the public chat, which everyone on the call can see and participate in.

General Data Protection / Cyber Security

- As part of the COVID-19 response a number of template Data Protection Impact Assessments (DPIA) have been written for Zoom, Slack and Dropbox etc. The DPIA will need updating with your organisational details and how you are using it etc. Contact us for further information.
- In terms of security Zoom has also released a statement addressing some of the issue brought up in the media.
- Salford CVS administer the GM VCSE Information Governance Group – We are sharing weekly updates on legislation and updates etc. If you have a member of staff responsible for Information Governance / Data Protection that you want adding to the group please email marie.wilson@salfordcvs.co.uk