



Best Practices for Securing Your Virtual Zoom Classroom



Lock Your Virtual Classroom

You can lock a Zoom session that has already started so that no one else can join. This is similar to closing the classroom door after the bell has rung. You can give students a few minutes to join the session and then click the Participants button at the bottom of your Zoom window and select "Lock Meeting" from the pop up menu.

[How to Lock Your Classroom](#)

The default screen-sharing settings for education users are set to "Host Only," so only teachers can share content in a session. Teachers can allow screen sharing in the host controls if students need to share their work with the session.

[How to Manage Screen Sharing](#)



Control Screen Sharing



Enable the Waiting Room

To protect your virtual classroom from unintended participants teachers can enable the Waiting Room with the following options.

- All Participants: students will be sent to the virtual waiting area, where the teacher can admit them individually or all at once.
- Guest Participants: Anyone who is not signed in as a member of your class will be sent to the virtual waiting area.

[Secure Your Meetings with Zoom Waiting Rooms](#)

As the session host the teacher can control who students are allowed to chat with. Chat access can be controlled from your in-meeting toolbar controls so students can still interact with the teacher and guests as necessary but not privately message other students.

[Controlling and Disabling In-Meeting Chat](#)



Lock Down the Chat



Remove a Participant

You can remove uninvited participants who have joined your virtual classroom by hovering over their name in the Participants menu and selecting "Remove from your virtual classroom". These participants will not be allowed back into the session.

[Managing Participants in a Meeting](#)

Privacy Requirements when using Zoom

- Disable "Join before host" - turned off by default
- Disable "File Transfer" and use Office Class Notebook or Google Classrooms to share files instead. - turned off by default
- Disable "Allow removed participants to rejoin"- turned off by default
- Keep "require meeting password" - turned on by default
- Do not share links to meetings on Social Media- this makes the meeting public
- Avoid using your Personal Meeting ID (PMI) to host public events.



Security Options



For details visit [Best Practices for Securing your Virtual Classroom](#)

