

# CHESTER COUNTY INTERMEDIATE UNIT

## Zoom Security Guide

### OVERVIEW

The Chester County Intermediate Unit (CCIU) is pleased to provide this supplemental resource to our schools and districts to complement Zoom training. Due to the increased use of the Zoom meeting platform in the wake of school and business closings and stay-at-home orders, a new disturbing phenomenon has surfaced called “Zoombombing.” Zoombombing occurs when uninvited, malicious participants surreptitiously enter a Zoom meeting and use the platform to display inappropriate content or harass participants. Intruders can also maintain a low profile during the meeting and intercept sensitive data. This is especially troubling as resourceful educators are understandably seeking to employ Zoom as a way to engage students in online learning.

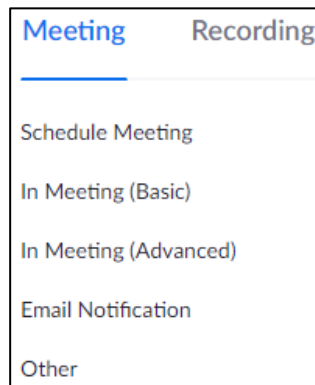
This guide outlines some steps you can take to make your Zoom meetings more secure as you deliver continuity of education. You may turn the settings noted below on or off to suit your particular needs. Please be sure to consult with the policies established by your school or district and confer with your internal IT staff if you have questions about implementing these or other measures.

### ENHANCING YOUR ZOOM SECURITY: ACCOUNT SETTINGS

These measures can help prevent unwelcome participants from entering your meeting or limit their activity if they do. Find additional information from Zoom [here](#).

#### Changes to Account Settings:

These changes can be made by going to <https://zoom.us/profile/setting> and signing into your account, then clicking *In Meeting (Basic)* at the right.



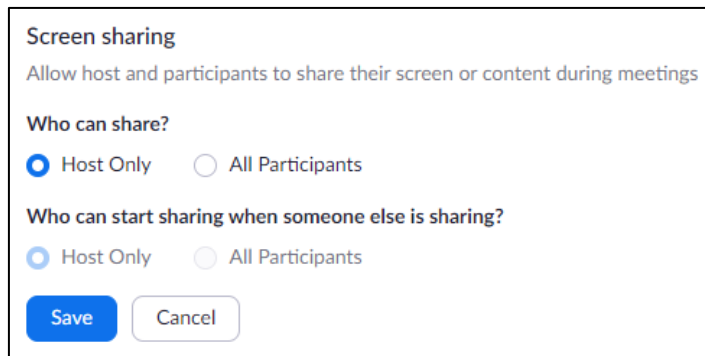
#### 1. Prevent Participants from Screen Sharing

Intrusive participants can share inappropriate content on their screens.

Limiting the screen sharing feature to “host only” helps to eliminate this possibility.

To restrict screen sharing:

- Under *Screen sharing* find *Who can share?* and select *Host Only*
- Click *Save*



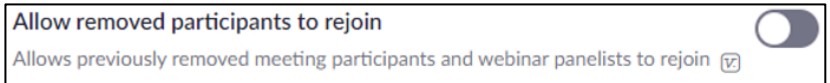
An equal opportunity employer and educator

The suggested account changes below can be made by simply ensuring that the associated function is toggled off in the *In Meeting (Basic)* menu.

## 2. Prevent Removed Participants from Rejoining Meetings

If an intrusive participant is removed from the meeting, they will be able to rejoin unless prevented from doing so.

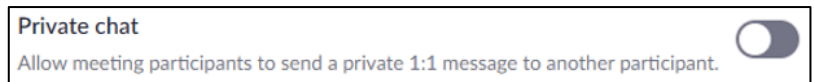
To prevent removed participants from rejoining, ensure that *Allow removed participants to rejoin* is toggled off.



## 3. Disable Private Chat

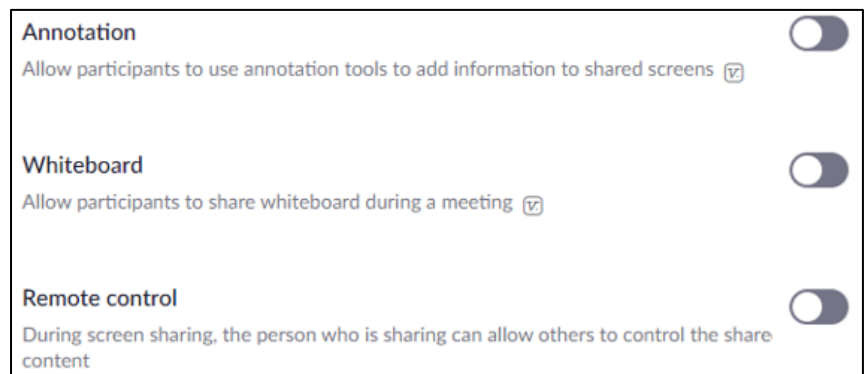
Private chat allows participants to send chat messages to only one participant.

Disabling this feature will not prevent an intrusive participant from sending chats, but since their chats will be visible by all participants, it will make their activity more detectable so that they can be removed more quickly. To disable private chat, ensure that *Private chat* is toggled off.



## 4. Disable Annotation

Intrusive participants may share unwanted text on a host's shared screen. To disable annotation, ensure that *Annotation* is toggled off.



## 5. Disable Whiteboards

Intrusive participants may share inappropriate content on a personal whiteboard.

To disable whiteboards, ensure that *Whiteboard* is toggled off.

## 6. Disable Remote Control

Intrusive participants may attempt to gain control of a shared screen. While control requires acknowledgement of the request from the screen sharer, disabling this feature helps avoid an inadvertent transfer of screen control. To disable remote control, ensure that *Remote control* is toggled off.



## ENHANCING YOUR ZOOM SECURITY: BEFORE THE MEETING

The best way to implement the following setting adjustments is by logging in to your online Zoom account at <https://zoom.us/signin> and clicking *Schedule a Meeting*. If you've already scheduled the meeting and want to edit the settings, click on *Meetings* at the left, choose the meeting you want to update and click *Edit*. Find additional information from Zoom [here](#).

SCHEDULE A MEETING

### 7. Generate a Unique Meeting ID

Hosts must provide participants with a 9- or 10-digit ID number or a meeting URL when inviting them to a session. You have the option of using the personal ID/URL associated with your account or generating a unique one. Especially if you are posting the meeting in a public forum (e.g., website) or if one of your previous meetings was compromised, it is recommended that you use a unique ID. While this is slightly less convenient than using a familiar, personal ID/URL, it can help to lessen the chance that an intruder will compromise your meeting. To generate a unique ID:

- In the *Meeting ID* section, choose *Generate Automatically*.
- Do not select *Recurring meeting*, even if your meeting is part of a series.\*
- Click *Save*. You will receive confirmation of your meeting with connection information for your participants, including your unique URL & ID, which you can copy for email or open with a calendar.

Meeting ID ☒ Generate Automatically ☐ Personal Meeting ID

☐ Recurring meeting

\*Note: If your meeting is part of a series, then you'll need to schedule a new meeting for each session. You cannot change an existing meeting's ID.

### 8. Require Participants to Register

You can configure your meeting so that participants must register for meetings through a custom URL that Zoom generates for you. To register, participants must enter their first name, last name and email address. To join, a participant's credentials must match those they used to register.

To enable registration:

- In the *Registration* section click *Required*.
- Click *Save*. In the *Invite Attendees* section, you will see a registration link for your participants. From there, you can copy the meeting invitation to email or to a calendar invite.

Registration ☒ Required

Invite Attendees

People are required to register before joining this meeting.

Registration URL: [https://example.zoom.us/meeting/register/abcde--ffgHI1j\\_kLm2opqRsTU3wxy4ZZ](https://example.zoom.us/meeting/register/abcde--ffgHI1j_kLm2opqRsTU3wxy4ZZ)  Copy the invitation



An equal opportunity employer and educator

## 9. Require a Password

Meeting Password ☒ Require meeting password 123456

You can further restrict access to meetings by requiring your participants to enter a password to join. To require a password:

- In the *Meeting Password* section, check *Require meeting password*. In the resulting text field, enter the password you want or accept the one that Zoom generates.\*
- Click *Save*.

\*Note: When creating meeting passwords, keep in mind that some videoconferencing equipment can only enter numbers. If some participants connect from videoconferencing hardware instead of a computer or mobile device, a numerical password should be used to ensure that they can connect without issue.

## 10. Mute Participants upon Entry

You can configure your meeting room so that every participant's audio feed is disabled when they first join. However, participants can enable their audio when they choose. To ensure that participants are muted when entering the meeting:


- In *Meeting Options* check *Mute participants upon entry*.
- Click *Save*.

## 11. Enable the Waiting Room

Enabling the waiting room prevents participants from joining the meeting until you admit them. This allows you to scan participant names and deny entry to any that appear suspicious. To enable the waiting room:

- In *Meeting Options*, check *Enable waiting room*.
- Click *Save*.

Meeting Options

- ☐ Enable join before host
- ☒ Mute participants upon entry 
- ☒ Enable waiting room
- ☒ Only authenticated users can join: Sign in to Zoom

## 12. Require Participants to be Logged into a Zoom Account

You can require all participants to be logged into their own Zoom accounts before accessing your Zoom meeting room. While this setting does not discriminate between institutions providing Zoom accounts (that is, it cannot restrict the meeting to accounts provided by your school or district), this is an additional precaution you can take to restrict access to your meeting. To require participants to log in:

- In *Meeting Options*, check *Only authenticated users can join*. *Sign into Zoom* will appear at the right.
- Click *Save*.



### 13. Turn Off Participant Video upon Entry

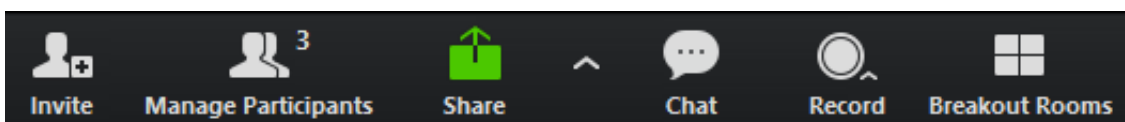
You can configure your meeting room so that every participant's video feed is disabled when they first join. However, participants can enable their video when they choose. To ensure that participants enter the meeting with their video off:

- In the *Video* section select *off* to the right of *Participant*.
- Click *Save*.



## ENHANCING YOUR ZOOM SECURITY: DURING THE MEETING

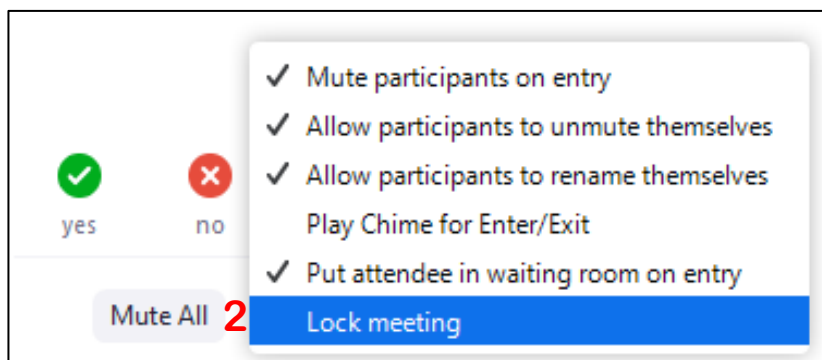
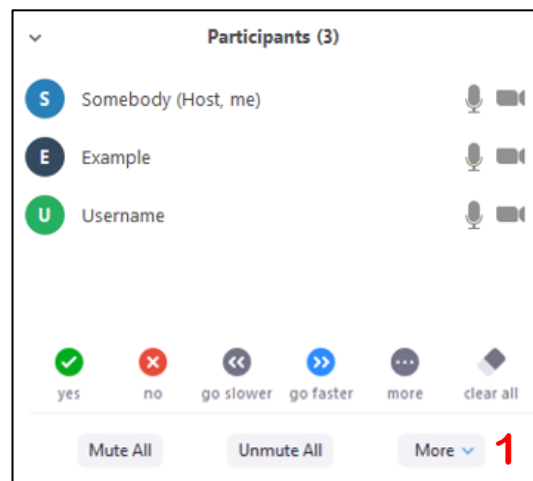
The following measures can help mitigate the impact of an unwelcome visitor or uncooperative participant after the meeting has begun. To implement these measures, click *Manage Participants* in the Zoom toolbar. The *Participants* window should appear on the right. Find additional information from Zoom [here](#).



### 14. Lock the Meeting

Locking a meeting prevents any new participants from joining. To lock your meeting:

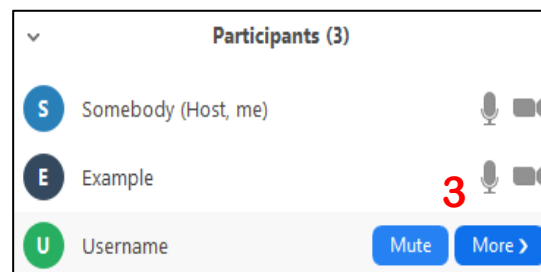
- Click *More* **1** in the bottom right-hand corner.
- Click *Lock Meeting*. **2**



## 15. Remove the Participant

To remove a participant from the meeting:

- Hover over the name of the participant and select *More*. **3**
- Click *Remove*. **4**
- Confirm by clicking *OK* in the resulting window.



## 16. Stop the Participant's Video

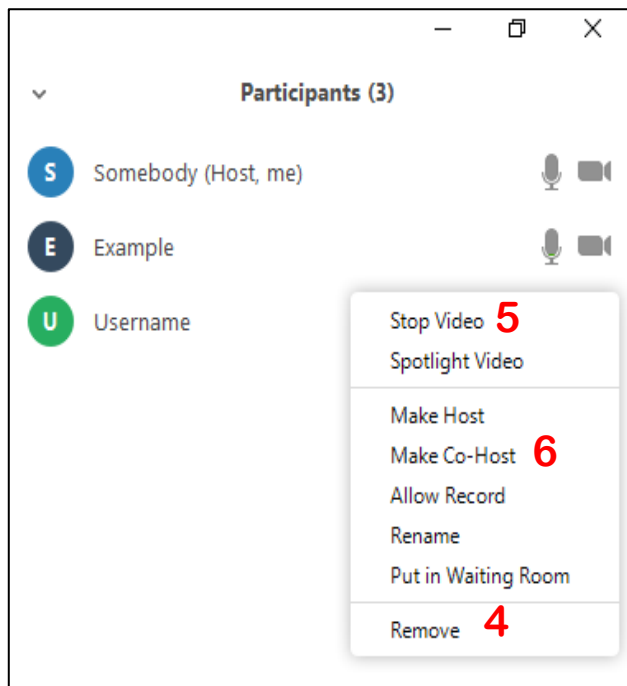
To disable a participant's video feed:

- Hover over the name of the desired participant and select *More*.
- Click *Stop Video*. **5**

## 17. Designate a Co-Host

Depending on the size of your meeting, it may be difficult to both run your session and moderate your participants. A second host can help with these responsibilities while you conduct your meeting. To delegate host privileges to an additional person:

- Hover over the name of the desired co-host and select *More*.
- Click *Make Co-Host*. **6**



*For questions, comments, or concerns, please contact:*

Bryan Ruzenski  
Director of External Technology Services  
Innovative Educational Services  
Chester County Intermediate Unit | CCIU #24  
bryanr@cciu.org  
484-237-5026  
Zoom: <https://cciu.zoom.us/my/bryanr>



An equal opportunity employer and educator