Gateway Public Schools Best Practices for Using Zoom with Students

Due to the recent “Zoom bombings” experienced by other schools, organizations and businesses, Gateway has instituted best practices for using Zoom with students. While we have not experienced a “Zoom bombing” at Gateway, we are taking precautions now to ensure students and teachers can use the platform for office hours and classroom instruction without interruption.

The following best practices are not exhaustive of all of Zoom’s capabilities and their security updates are occurring daily. Faculty and staff are encouraged to read the latest updates as they are released by email. If you have any questions about how to implement any of these security tools, please reach out to your school site leadership for support.

Host starts the meeting

When setting up meetings, teachers should use the default setting of hosts starting the meeting. This means students cannot join the meeting before the teacher has “arrived.” Students will see a pop-up box that says, “The meeting is waiting for the host to join,” which provides additional control and security for meetings.

Waiting Rooms

Faculty and staff use the default Waiting Room setting. This allows the host – teachers – to control when a participant joins the meeting. This is the best way to control who is entering Zoom meetings by giving teachers the option to admit participants individually. This allows teachers to ensure only students are entering the Zoom meeting room and prevents outside, unwanted participants. Learn more about the Waiting Room feature here.

Signed-in Users Only

When possible, teachers should allow authorized users only into Zoom meetings. This means setting up the Zoom meeting with the email addresses of students who should have access to participate in the meeting. Anyone else who tries to join the meeting will be declined. Instructions for setting up “authenticated users only” settings can be found here.

Meeting Passwords

Meeting passwords are an added level of protection for Zoom meetings and are now a default setting for Education Zoom accounts. Passwords for meetings can be used at the discretion of teachers as passwords may be an access barrier for some students.

No Video and Mute Upon Entry

Meetings should be set up with the default setting of no video/mute for all participants. Teachers will turn students' microphones and video on once participants have been approved to join the meeting. This helps to indicate the start of office hours/classroom time.

Restrict Screen Sharing

Screen sharing should be done only by teachers and staff. Giving up control of the screen can expose students to unwanted content. Before starting a meeting, teachers and staff should change their screen sharing settings to “host only” using the meeting set-up controls or at the bottom of the Zoom screen once the meeting has started. Step-by-step instructions available here.

Lock the Meeting

Once everyone has joined the Zoom meeting who should be present, the host (teacher) will lock the meeting. This disables anyone else from joining. Understandably, this cannot be used during office hours as they have an “open door policy” for students.

Removing Participants from a Meeting

If an unwanted guest manages to join the meeting after all of these precautions are taken, or if a student is not following the class’ norms, the teacher will remove participants manually. Once they have been removed, they cannot rejoin the active meeting. If the wrong student or person is accidentally removed, teachers can allow participants to rejoin using these instructions.

Disable Private Chat Feature

Teachers should disable the private chat feature during office hours and other student-related Zoom sessions. This cuts down on distractions while teachers are engaging with students and prevents anyone from receiving unwanted messages during the meeting. Instructions for changing chat permissions available here.