Zimbra **chinn@4j.lane.edu**

[4j_priority_mail] UPDATE: Secure Video Meetings with Zoom

From : Kerry Delf <delf_k@4j.lane.edu> Thu, Apr 16, 2020 12:39 PM
Sender : 4j_priority_mail <4j_priority_mail-bounces@4j.lane.edu>
Subject : [4j_priority_mail] UPDATE: Secure Video Meetings with Zoom
To : 4j priority mail <4j_priority_mail@4j.lane.edu>

Dear colleagues,

Security concerns about tools for online meetings have been in the news recently. As we all transition to online teaching, learning, working and living, we must be mindful about the online tools we are using.

District staff are using Zoom for many face-to-face meetings from a distance. Zoom is a secure environment, but only when the available security features are used. It is important for you to know that there are valid concerns about security if the meeting organizer does not take certain simple security steps.

Safety is always our priority. Our 4J technology team has created training documentation for Zoom security practices and how to set up your settings, and is exploring additional security measures and options.

Following is a reminder of some things to keep in mind to ensure your Zoom sessions are safe and secure, with a couple of additions to these guidelines we previously shared last week. Though the detailed settings may differ, these general practices also apply to other platforms.

A few of the most important are:
• **Do not make meetings publicly accessible** or post the link or password anywhere that is open to the public, including a calendar.
• **Confirm participants' identity**. Really check and be sure you recognize each participant before you admit them from the waiting room.
• **Do not record meetings**.
• **Keep up-to-date with software updates.**

If you have questions about this or other technological issues, please talk with your supervisor or contact the Technology Department (see below). Thank you!

Key expectations and tips for all users:

• **Accept software update prompts from Zoom**. Zoom is actively pushing out updates to address any issues or vulnerabilities, and it's important for us to be on the forefront of updates.
• **Use your 4J email to set up your Zoom account**. Never use a personal email.

• **Do not make meetings publicly accessible.**
• Do not record video meetings with other employees.
• **Do not record** classroom sessions or meetings with students. (There may be some exceptions – please talk with your supervisor). Do encourage and expect that your students adhere to this guideline as well.
• You may video-record yourself covering lesson content and make that content available to students, but you should not record students.
• Do not share screenshots of video meeting participants or post them on social media, and teach this expectation to students as well. This goes for both classroom meetings and staff meetings.
• Be aware of what is in your camera background. Project a professional image.
• Close all unnecessary windows before sharing your desktop.
• Use one-on-one video conferencing with students only when there is a clear educational purpose and necessity. Examples include conferring with a student during office hours, or providing special education or other student services for which one-on-one communication is required. Do transparently communicate with a student's parent when using one-on-one video conferencing, just as you would for texting or emailing.

If you are organizing Zoom meetings:

• **Familiarize yourself with Zoom's settings and features** so you understand how to protect your virtual space.

• **Generate meeting IDs automatically**, using a unique meeting ID and password each time. Do not use your personal meeting ID—anyone who has your personal meeting ID link can join any meeting that also uses that link.

• **Require a password** when you schedule and set up your Zoom meeting, and do not post it anywhere that is publicly accessible. (This is now the default setting for new meetings set up in Zoom.)

• **Do not post a link to your Zoom meeting** anywhere that is publicly accessible, such as a website, social media, or publicly shared online calendar. Anyone who has the link can join your meeting.

• **Create a "Waiting Room"** when you set up your Zoom meeting (it's now the default setting) and actively use it to ensure only authorized participants join your meeting. Participants will be staged in the waiting room and you will allow participants into the meeting individually and/or in bulk. Make sure you recognize each participant before you admit them from the waiting room. If you have any students who will be joining via telephone, know their phone number in advance and only admit callers with recognized phone numbers. Keep in mind that if a participant leaves and comes back, they will need to be reauthorized.

• **Be present from start to end in every meeting**. Select "Require host to be present before meeting starts" setting when you schedule and set up your meeting in Zoom. Be the last person to hang up and end the video conference.

• **Mute participants on entry** and enable audio and video only when you are ready.

• **Keep control of the screen share setting** and (for students) disable private chat. The screen sharing default is now "host only." If at any time during the meeting you want a meeting participant to share their screen, you can enable it during the meeting.

• **You can "Lock" a meeting** once your meeting is started and all the participants you are expecting have joined. You can find this setting under: Participants >> More >> Lock Meeting.

• **As the meeting host, you have the control** to mute participants, expel a participant, or stop the meeting, if there is a problem. Hover over the participant's name, or click the ellipsis (...) near their name, and click the remove button.

For more tips on Zoom meeting security and safety, see:

4J Technology: Zoom Privacy Considerations — Guidelines and step-by-step instructions for Zoom settings
https://www.4j.lane.edu/wp-content/uploads/2020/04/4J_Technology_ZoomBestPractice_v1.3.pdf

Zoom: Best Practices for Securing Your Virtual Classroom
https://blog.zoom.us/wordpress/2020/03/27/best-practices-for-securing-your-virtual-classroom/

Zoom: Keep Uninvited Guests Out of Your Zoom Event
https://blog.zoom.us/wordpress/2020/03/20/keep-uninvited-guests-out-of-your-zoom-event/

Key 4J Policies:

IIBGA-AR Technology Appropriate Use: http://policy.osba.org/eugene/I/IIBGA%20R%20D1.PDF
IIBGA Electronic Communications System: http://policy.osba.org/eugene/I/IIBGA%20G1.PDF

If you have technology questions:

4J Technology Helpdesk, 4Jdesktop@4j.lane.edu, 541-790-7777

Thank you for your attention to provide a secure meeting and learning environment for all of our staff and students!

Best wishes,

--
Kerry Delf
Chief of Staff
Eugene School District 4J
delf_k@4j.lane.edu | 541.790.7733

You received this message because you are subscribed to the 4J list: 4j_priority_mail.
