AL ROWAD BRITISH PVT SCHOOL

Cyber safety Instructions

Instruction for Teachers:

If you are hosting a Zoom meeting, here are a few things to look out for to be safe online:

1. A public meeting link is public so do not share it with anyone you do not trust.
2. The same with your personal meeting ID. This is like a personal phone number that people can “drop in” on at any time. Make sure to set up a password for participants to verify their entry before accessing the Zoom meeting.
3. When you are in the meeting, you will need to manage screen sharing by ensuring you are the only person in control of the meeting. To do this, click on “Who Can Share?” and confirm that “Host” is the only button clicked.
4. Manage participants by ensuring only signed-in participants can join all. This way you know who people are if they are behaving badly.
5. Set two factor authentications, remove unwanted or disruptive participants. You can report unwanted activity, harassment and cyberattacks to Zoom directly.

Instruction for Students:

If you are a participant in a Zoom meeting, the Host of the call may have more powers than you think:

1. Be aware that the host can record the call - if you see a small red dot the call is being recorded.
2. Ask why your host is recording and where that information is being stored. Recorded content should be stored on a secure server to protect from unwanted and unauthorised use of video content.
3. Know that hosts can use the built-in “Attention Tracking” tool, which will allow them to know if you have clicked off Zoom and into another browser window for more than 30 seconds. This is not evident to non-hosts.
4. Consider your personal room privacy and security as well. You can use a virtual background to avoid sharing unnecessary information about your personal space, such as books, posters, windows or any other details that give off information about your preferences, habits or the location of your home.
5. Turn off your microphone and camera when you are not speaking to avoid unwanted tracking of your responses or actions.

Instruction for Parents:

Tips if your child or teen is using Zoom:

1. If your child is using Zoom to participate on classes with their teacher, you can expect that the teachers will have put in place precautions such as two-factor authentication with a meeting ID and user password and locking the session so that no new participants can join. If you have concerns, check in with the teacher to see if the session is password protected and the class secure.
2. If your child or teen is using Zoom to chat/meet with friends, take the time to ensure that they understand how to use the App safely and that they are familiar with the security features.
3. Remind your child, that as with any App or online facility, they shouldn't be video chatting with strangers or people they don't know in person and that they should never join a meeting or accept a request from someone you don't actually know.. Also remind them that they should avoid saying or doing anything on video that they would not feel comfortable having shared outside the group.
4. Make sure you and your child consider what background is visible when they are on zoom so as the privacy of other family members and the security of the home is protected. For example, consider using a Zoom virtual background such as Minecraft so that messy rooms or family living areas are not visible in the background.
5. Explain in an age appropriate way what 'Zoom bombing' is and instruct them to tell you or another trusted adult if something happens online that makes them feel scared or uncomfortable.
6. As with any online activity, it is important for parents to monitor their child's video chats. That does not mean hovering over their shoulder all day - but it does mean keeping an eye and an ear out at frequent intervals. And now, more than ever, be sure to keep all devices out of bedrooms.