ZOOM BEST PRACTICES AND GUIDANCE

NOTE:

The DC Government standard tools for teleconferencing are WebEx and Microsoft Teams, we do not encourage or support Zoom.

But we are aware that some vendors and schools are using Zoom, if it is unavoidable please follow these best practices:

Below are basic security measures which can be applied by going to "Settings", select "Meetings", then:

1. **Do not make meetings or classrooms public**. In Zoom, there are two options to make a meeting private: require a meeting password or use the waiting room feature and control the admittance of guests.
2. **Do not share a link to a teleconference or classroom on an unrestricted publicly available social media post**. Provide the link directly to specific people.
3. **Add a passcode** to your meeting, then share that passcode with your guests. Once set, the passcode is required in order to enter the meeting.
4. **Manage screensharing options**. In Zoom, change screensharing to "Host Only."
5. **Ensure** users are using the **updated version** of remote access/meeting applications.
6. **Consider turning on the "waiting room**" for your meeting so that you can scan who wants to join before letting everyone in.
7. **Deselect "Join Before Host"** if you don't want participants to join/interact before the host enters. Set an alternate host if you need a backup host.
8. **Disable "Allow Removed Participants to Rejoin**" so that participants who you have removed from your session cannot re-enter.
9. **Disable "File Transfer**" unless you know this feature will be required.
10. **Designate someone** who is not actually participating in the conference as a "co-host" so they can monitor the traffic and remove troublesome participants, if necessary.

These practices may seem a bit much, but it's better to be prepared.