

## Zoom – Safety and security

Zoom has proved to be a great tool for conducting business during the Covid-19 Pandemic. Below are some of the practices the District is taking to ensure the safety and security of meeting participants as well as some tips for how you can keep yourself secure.

### Steps the District is Taking

- All public meetings have a staff member present acting as meeting host. The meeting host monitors participants as they enter and exit, monitors the chat, and has a number of special privileges that can be and are used to increase the security of the meeting. Those privileges are:
  - The ability to admit participants from the digital waiting room into the meeting. This allows the meeting host to reject admission to obviously nefarious participants and that participants cannot simply join a meeting themselves.
  - The ability to mute any participant at any time.
  - The ability to revoke another participants' screen sharing privileges.
  - The ability to remove a participant from a meeting at any time.
- The District is keeping Zoom software up to date. Outdated software can be more vulnerable to bad actors.
- District staff are staying abreast of best practices and technologies when it comes to safety and security on video conferencing platforms.

### Steps you can take

- Be aware that when you join a meeting, your camera and microphone might automatically be turned on.
- Be aware that some public meetings, such as meetings of the Board of Managers are being recorded by the District meeting host.
- Be aware that the chat record will be available to the District meeting host after the meeting has ended. Send chats accordingly.
- Before sharing your screen, check to make sure you don't have any sensitive documents, webpages, or other things open.
- Don't click links in the chat that come from unknown participants.
- If you downloaded the Zoom software, keep your software up to date.

These tips have been adapted from those published by the Federal Trade Commission:  
[https://www.ftc.gov/news-events/blogs/business-blog/2020/04/video-conferencing-10-privacy-tips-your-business?utm\\_source=govdelivery](https://www.ftc.gov/news-events/blogs/business-blog/2020/04/video-conferencing-10-privacy-tips-your-business?utm_source=govdelivery)

- If you are wary of downloading the Zoom software, feel free to join meeting through Zoom in your browser or call in using a telephone (you will find an associated phone number in each meeting invitation).
- If you feel that your security is being actively jeopardized during a District Zoom meeting, please notify the District meeting host. You can do this verbally, through the chat (through remember the chat record will become public), via email ([blauer@rpbcwd.org](mailto:blauer@rpbcwd.org)), or phone (952-607-6481).

The District strives to make all who we interact with feel safe and secure in all meeting venues, be they in person or virtual. If at any time you have suggestions, questions or concerns about video conferencing please address them to B Lauer ([blauer@rpbcwd.org](mailto:blauer@rpbcwd.org); 952-607-6481).