Safe use of Zoom from ACC newsletter 3 Aril 2020

Zoom is a frequently used tool to deliver services via Telehealth. Being free, and almost universally accessible, it's an effective tool for communicating with clients when face-to-face consultations are not possible.

Today we're highlighting some useful security features and good privacy practices for hosts.

Maximising privacy and information security

Zoom's desktop application has greater security features for hosts than the Zoom app.

Before the meeting

- it's more secure to generate a random meeting ID instead of sharing a link in the invitation
- only send the meeting invitation to required people
- send the password for the call via a separate method
- allow only signed-in users to join the meeting
- disable the 'join before host' feature
- enable the waiting room feature
- advise participants in advance if the meeting will be recorded.

During the meeting

- confirm who is on the call before discussing sensitive information
- only accept or open attachments you're expecting from call participants
- lock the session once everyone you were expecting to join the meeting has joined (at the bottom of the participants panel in the meeting, click 'More' and then 'Lock Meeting')
- only allow remote control of the screen sharing session from a call participant you know and trust (not good practice for webinars)
- use only the local recording feature in Zoom for video or audio records.

More information about Zoom host controls can be found on Zoom's website.

After the meeting

It's good practice to upload recordings to your system as soon as practicable.

Inviting ACC to Zoom meetings

ACC staff can be invited into video conferences where required, however this will be via audio and we won't enable video unless this is part of our normal role.