Coronavirus Pandemic

Information Security Measures – Using Zoom

This document provides guidelines on how to use Zoom securely as a conferencing tool during the current pandemic and increased home working.

It does not cover Council policy or requirements for conferencing with this mind you must ensure you are conversant with the Using Web Conferencing during Pandemic guidelines.

Security Measures - How to stay secure on Zoom

- do not share the link or the meeting ID on public platforms;
- ensure all invited persons are aware not to share the meeting ID with other parties and the need to retain it securely;
- do not share photos of the meeting i.e. by taking a screen grab or photo of the screen;
- never use the personal meeting ID, instead allow Zoom to create a random number for each meeting;
- for regular meetings issue a new ID each time;
- add a meeting password ensuring it is a sufficiently complex password/passphrase;
- set screen sharing to "host only";
- disable file transfer;
- disable "join before host";
- disable "allow removed participants to rejoin";
- do not access URL's (web site links) or drive links provided within chat windows and advise all attendees not to share these via the chat window. If sharing of URLs (web site links) or drive links is required do this via another means such as email.

What is Zoombombing

Zoombombing is where uninvited guests attend a zoom meeting mainly with intent to disrupt, cause upset or steal information / files.

Council staff attending Zoom meetings must ensure the above security measures are in place.

Malicious actors attempt to get into Zoom meetings in various ways:

- Already knowing a meeting ID for connecting – if meeting is password protected it makes access more difficult or indeed impossible if password / passphrase is suitably strong;
- By randomly entering nine digit numbers until one matches a zoom meeting ID. This can be done manually or automatically using a random generating tool - if meeting is password protected it makes access more difficult or indeed impossible if password / passphrase is suitably strong