Information Security

Staff Guide on the use of Zoom on council managed devices
February 2022

Please note that our **preferred and approved video conferencing platform** is, and continues to be, Microsoft Teams – this should be your default option unless you have an essential business reason that you need to use Zoom.

In these essential, limited circumstances, Zoom can be used across council managed devices for your video conference – providing all the rules below are followed.

Please be aware that Zoom is only accessible to staff with Level 2 internet permissions and above (for internet permissions at level 2 or above you need to contact your line manager for approval). Zoom can only be used via the internet browser version – the current restrictions on installing the app remain in place.

Rules when using Zoom

- ✓ You must have the **correct internet permissions** to use Zoom – level 2 minimum.
- ✓ You must have a **genuine business need** to use Zoom as your video conferencing solution.
- ✓ You must **not use Zoom for personal use** on a council device.
- ✓ You must **not set up a Zoom meeting** yourself- if you need to create a meeting you should use Teams.
- ✓ You are only **permitted to join a Zoom meeting set up by a third party** – individual or organisation.
- ✓ You **must not discuss sensitive** matters when using Zoom – this is any content that you would normally protectively mark as OFFICIAL - SENSITIVE when creating, saving, printing or sharing it.
- ✓ You can only use Zoom on an **internet browser** when using a council device.
- ✓ You are **not permitted to record** a Zoom meeting when using a council device.
- ✓ If you are in contact with the Zoom meeting organiser, to help keep you protected, you should check if they have **set up your meeting securely by** being aware if they are**:**
  - o using the Waiting Room feature to see who is attempting to join the meeting before allowing access.
  - o using a different ID for each meeting-– suggesting that the organiser does not use the same meeting ID for all their meetings and does not share the ID.
  - o using a password to protect the meeting.
  - o managing the meeting participants - by checking whether there is only one host to control the meeting and that the host understands how to control participants, screen-sharing, camera, and mute options.
- ✓ You are not permitted to **use any of Zoom's more amusing features** such as inverting participants' images or adding "bunny ears" for example when participating in a business meeting on Zoom on a council device. This is not appropriate conduct for business activity and should be avoided.
- ✓ You **must not download** any content to your work device that is shared with you on a Zoom meeting – this is because it does not go through the same level of security measures and could contain malicious software that can affect and damage our network.