**Zoom Security Guidance – Work and Personal Use**

**Purpose**

1. This guidance sets out SGUL’s advice to staff on important security settings when using Zoom remote conferencing services. This guidance sets out the recommended security measures individuals should take when using Zoom.
2. The guidance covers both work and personal use of Zoom.
3. Zoom is not to be used to host SGUL related meetings but can be used to attend Zoom meetings.
4. Under no circumstances when using Zoom should information containing Personal Identifiable Data and sensitive data be discussed or used.

**Context**

1. This guidance applies only during COVID-19. In normal circumstances SGUL would have conducted security reviews and accreditation and assurance processes for the technology in use. Due to the exceptional circumstances as a result of COVID-19 we are relaxing these requirements for video conferencing where MS Teams cannot be used.
2. If Microsoft Teams can be used then it must be used. You will still need familiarize yourself with this advice as you may be asked to join a Zoom meeting when engaging with other agencies.

**What is Zoom?**

1. Zoom provides a video and audio-conferencing toolset, based on the premise of joining meetings from anywhere, on any device, at any time. This functionality allows for increased remote working capability, collaboration, and video calling functionality for practically all situations a staff member might attend or chair a meeting for.

8. There have been security issues with Zoom over the past 18-24 months and it is not risk-free. If you are going to use Zoom, you need you to follow this advice and help protect SGUL’s information during these unprecedented times.

**Our advice when attending a meeting using Zoom for SGUL or personal use.**

9. Zoom Access:

1. For SGUL use you should only use Zoom’s in-browser functionality and certainly do not use the Zoom smartphone app.
2. For personal use on your own personal laptop (non-SGUL work) we would recommend using Zoom’s desktop application or the in-browser functionality (from a laptop or mobile device)

10. There has been public reporting about Zoom’s record of enabling user tracking on its

mobile applications, and a permissive privacy policy. If you are on a mobile device you should use Zoom’s in-browser option. Note that when joining a Zoom on mobile, Zoom will try to guide you to download the app instead of proceeding to use it in the browser. As per figure one (below) there will be smaller text “join from your browser”. Click on this link, sign in and join the meeting this way. However, this may not be possible on all mobile platforms.

Figure one: Zoom joining screen on mobile phone1



11. We recommend that all users enable multi-factor authentication (MFA) on Zoom accounts, however at present Zoom is only able to provide MFA to its web browser users. MFA does not apply to the Zoom desktop client or mobile app.

**Personal use of Zoom only**

**Hosting a meeting using Zoom**

12. The Zoom smartphone app must not be used for ***hosting*** meetings or presentations.

 15. You should use the Zoom desktop application to host calls or presentation.

**Setting up the meeting**

 16. When creating the invite and sending it out, you should:

1. generate a random meeting ID, rather than sharing a link
2. allow only signed-in users to join the meeting
3. disable the “join before host” feature
4. enable the waiting room feature
5. only send the meeting invite information to required people
6. send the password to the call via a separate method (i.e. send the meeting invite information via an email and the password via telephone call).

 17. If recording of the video or audio is required, then the local recording feature within

Zoom must be used.

**Once the meeting has started**

 18. When you start to host the meeting:

1. check who is on the call before information is discussed
2. only accept/open attachments you are expecting from call recipients
3. only allow remote control of the screen-sharing session from a call recipient you know and trust (note that this feature should not be used in a webinar scenario)
4. lock the session when 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”).
5. More information about Zoom host controls can be found here: <https://support.zoom.us/hc/en-us/articles/201362603-What-Are-the-Host-Controls-.>