Document Control
Reference: BUL-GUI-ZOOM
Issue No: 2
Issue Date: 22/04/2020

Guidance - Using Zoom Securely

InfoSec and Data Protection guidance for Brunel staff using Zoom.

Mick Jenkins MBE - Chief Information Security Officer

Key Points

- Ensure *"Require meeting password"* is **enabled**. Passwords must use 10 digits; please ensure you distribute the password separately in a controlled manner.
- Ensure the *"File transfer"* feature is **disabled** - The sharing of files is not be permitted with Zoom, it should be exclusively for "face-to-face" meetings and screen sharing.

User Guidance

- Don't use social media to share conference links as malicious groups can search for these meetings.
- Apply the Acceptable Use Policy and the Information Classification Policy whilst using Zoom.
- Whilst in Zoom meetings do not continue to use AnyConnect VPN, use local Internet connectivity.
- Zoom collects data from users about devices, activities and data shared or transferred. The University Data Protection Officer (DPO) recommendation is to only accept the necessary cookies and turn off the optional cookies in browser settings or by the Zoom Cookie Preferences link on the Zoom homepage.
- The meeting host may record a Zoom meeting and store the recording, this is stored in the Zoom cloud based in the USA. Anyone intending to record their meetings must notify all those invited that this is going to be happening. It is the individual host responsibility to gain consent from all participants.
- DPO recommendation is that Zoom users opt out of advertising to reduce the amount of data that is collected, processed or sold. You can ask Zoom to opt out of certain advertising practices related to your Personal Data by clicking on the "*Do Not 'Sell'* My Personal Information" link.
- Once all the intended participants have joined, close the meeting to prevent anybody else from joining. Select *"Manage Participants"* and then click *"More"* at the bottom, Select *"Lock Meeting".* Allow only signed-in/Registered users to join: If someone tries to join your meeting and isn't logged into a Zoom account, they will receive the message 'This meeting is for authorised attendees only'.
- Prevent changing display names to hide/change identity, when in the meeting, go to Manage Participants panel, click *"More".* Ensure the *"Allow Participants to Rename Themselves"* is unchecked.
- Screen sharing is permitted, Limit screen-sharing ability to the host. change the default to set screen sharing to *"host only"* to prevent other meeting participants from sharing inappropriate screen shots.
- Disable virtual backgrounds to prevent someone from displaying an inappropriate image as their background. Choose *"Setting"* and select the *"In Meeting (Advanced)".* Disable the "Virtual background".
- Control when the meeting starts, don't let the participants join the meeting before the host. Use the "Waiting "Room" feature to have participants wait until the host arrives and vet participants prior to entering the meeting.
- Be aware of *this functionality: "Allow host to put attendee on hold"* in the "*In Meeting* (Basic)" section. This will allow the host to remove people from the meeting if necessary, owing to inappropriate behaviour.
- Ensure "Mute" is enabled when communication is not required. The presenter has the option to mute all the attendees and this should be used when conducting presentations.
- Use of the whiteboard feature where participants can annotate for all to see is permitted as long as *University Confidential information or sensitive personal data* is not discussed.
- Disable private chat: Restrict participants' ability to chat amongst one another.
- Do NOT use your Personal Meeting ID (PMI) when scheduling meetings. Allow Zoom to automatically generate the meeting ID is more secure and each scheduled meeting will have a unique meeting ID.
- **Staff are advised to utilise Teams and Skype for business when possible to reduce risks from Zoom use.**