Video conferencing: Using Zoom to carry out our work

Updated: 1st July 2020

Introduction

As more and more businesses are investing in, and using online video conferencing at this time, we are aware that this can increase the risks associated with its use, including the security of using their software.

Technology - both hardware and software – will never be 100% fault or security proof. But we always work to ensure that we mitigate, reduce or eliminate any risks when using technology and we spend a lot of time researching the right products to use – often paying higher costs and investing a lot of time to ensure we get close to 100% trust.

Our mission is to do good – not harm.

Using Zoom

In light of the potential risks with using specific platforms such as Zoom, we would like you to know that we are aware of the updated and emerging risks that have been identified.

We always work to ensure that we mitigate, reduce or eliminate any risks to our participants, clients and our own staff in all work we undertake, and the fast-shifting changes with digital and video conferencing are no different.

We follow and implement the features outlined in Zoom's security guide created in April 2020 (https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf) including (but not limited to): host authenticated meetings, password protected meetings, host controlled joining meetings, and in-meeting security (including encryption of all screen sharing content). By following and implementing these privacy features and best practice, we mitigate any potential issues.

When using Zoom, we ensure that participants only enter into a designated session with instructions provided directly by the facilitator, and only once the facilitator has started the session, to ensure participants are supervised and not left unattended using the platform at any time. When sending instructions to join a zoom session, we inform participants that registration details may become publicly searchable and that we therefore recommend minimal registration data is used. To join or register to join a session, participants only require an email address and we inform participants not to share any further details in registering. If we need to collect any participant details (such as demographic information) we do this separately before the zoom session via email or telephone communication.

We always start a session by explaining the *does and don'ts* for taking part in an online session. This ensures that we can instruct participants not to click on any links, pop ups or features that we are not directly talking to them about. We only send communications through Zoom sessions that are encrypted via the available encryption features.

When holding the focus groups and creative workshops, we maintain a strict control on the features that are enabled and disabled. Through the settings on our account, we do allow screen sharing, but for the host only and we disable the desktop / screensharing for users, along with the remote control feature. For features such as the annotation, whiteboard and nonverbal feedback, we determine which of these are required in the session and keep them enabled only if and when they are required (and not for the whole session). Other advanced features, such as the far end camera control, closed captioning and breakout room are disabled as a default in all sessions and are only activated on a case-by-case basis for any relevant part of a session. We make sure that the ‘file transfer feature’ default is switched off and we check that it is not activated at any point to minimise any potential risks posed by having this switched on.

We hold a paid subscription-based and private Zoom account [not free to use] which only designated account holders within our organisation are able to use to start and hold sessions. This enables us to completely minimise the way our account can be used and ensure it is only used for business-specific purposes (and not for purposes as such as violent imagery or other purposes). Having a paid account gives us better security features.

As the market offer for video conferencing and video calls are developing at a fast pace in line with the increased demand, we are continuing to explore other platforms that we could utilise which further minimise / reduce risks in their use. We are currently exploring MS Teams and Babl Cloud as potential alternatives, and assessing the balance of risk with the features to determine the most appropriate platform that can meet our security requirements and support our work.