

ESW Guidance for Remote Meeting Security

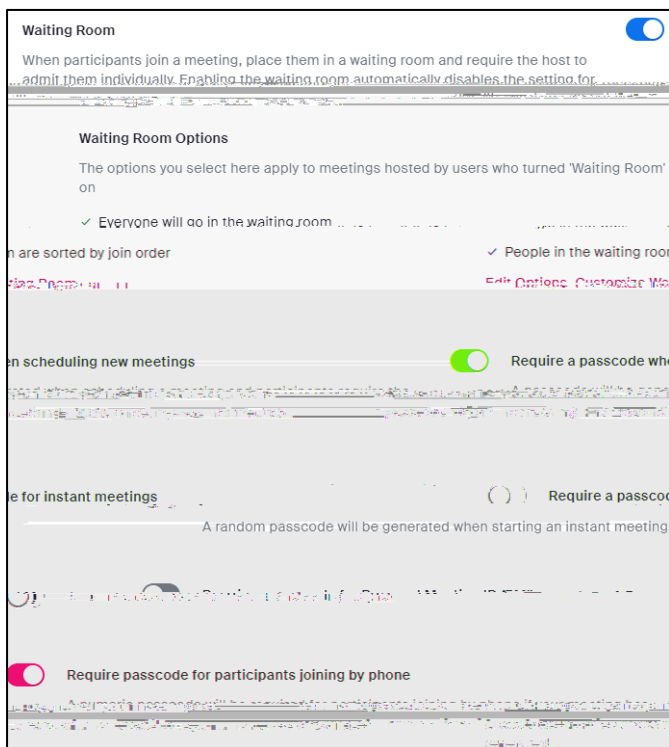
The University is committed to ensuring information security, including protecting itself from both deliberate cyber-attacks and accidental disruption to services.

The University has produced a [Stay Safe Using Zoom](#) guide. This includes a series of security settings you can use when setting up remote events using the Zoom platform.

A [Zoom Webinar](#) permits only specified panellists and an event host to talk, share their screen, turn on cameras, etc. Other attendees can only utilise the Chat function or Q&A box – both of which can be disabled by the hosts. Contact ITS for further details on how to set up this type of event.

In addition to Zoom's own guidance, the School of Education & Social Work provides the following advice to those planning or setting up remote events using the Zoom platform:

1. Consider having one person responsible for tech
2. It is not recommended you share Zoom links via social media, either directly within a post or via a link to a reg



Choose at least one of the following security settings:

Passcode (only for when sharing a link via password protected route, e.g. email or canvas -



If it is not possible to end the meeting for all, notify meeting attendees in the Chat to leave the meeting and access the [web-based version of Zoom](#) to end it from there.

When setting up a new meeting or event in Teams, click on the 'Options' icon to set security options.

Click 'More Options' to add

Any incidents of cyber-bombing on Teams should be reported [to ITS](#).

The [University's cyber security online training module](#) is mandatory for all staff

[Advice on Information Security](#) from the University of Sussex

[Top Ten Security Tips](#) from ITS at Sussex

How to ... Stay safe using Zoom from