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.

Zoom Security

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 se 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:

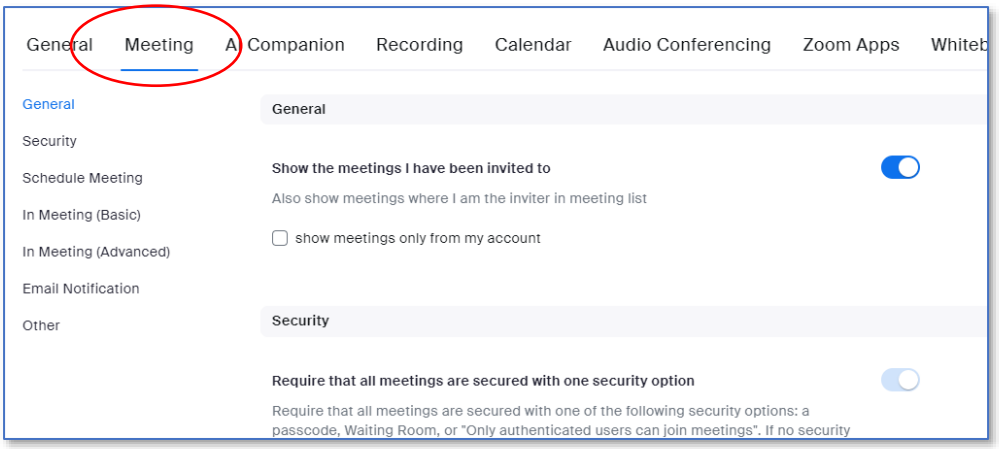
1. Consider having one person responsible for tech *only*
2. It is not recommended you share Zoom links via social media, either directly within a post or via a link to a registration form (e.g. Ticket Tailor, Eventbrite, Microsoft Forms, Google Forms etc.). Meeting attendees should be provided with the Zoom link close to the date of the event when hosts have had the chance to check registrants' details.

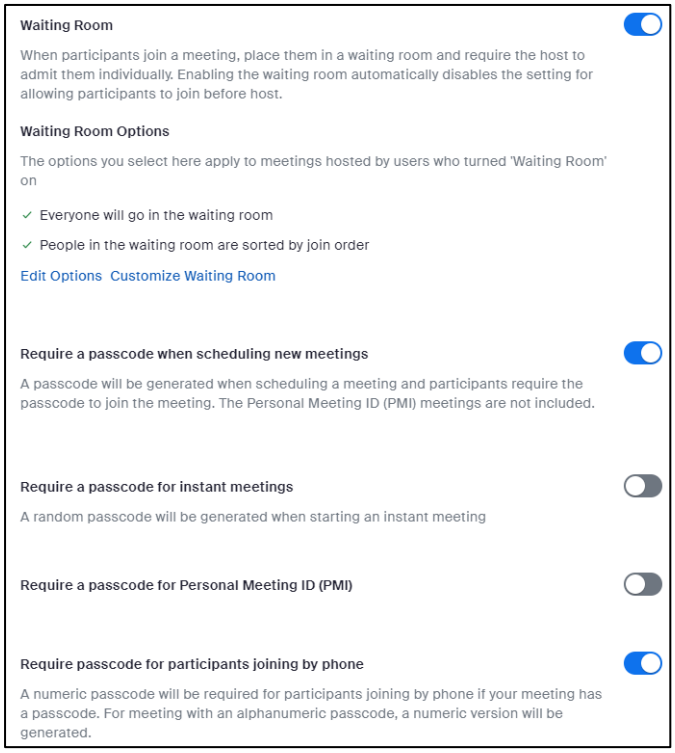
Security Settings for Zoom events

In advance of the event, you should:

- Go to the Zoom web settings: https://universityofsussex.zoom.us/profile/setting

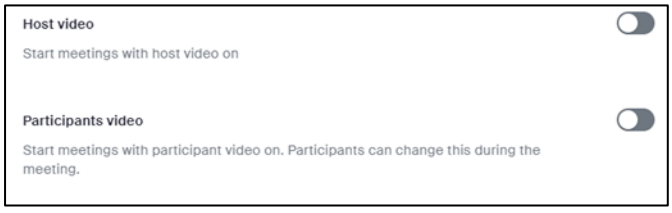
- Choose the 'Meeting' menu:



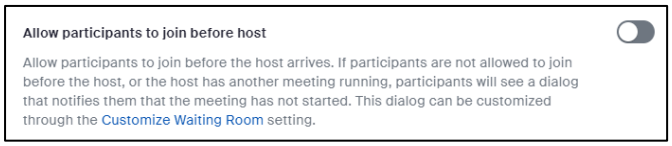


Choose at least one of the following security settings:

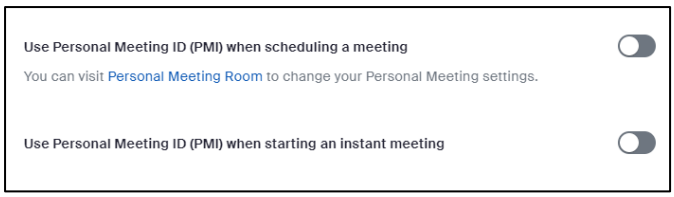
- Passcode (only for when sharing a link via password protected route, e.g. email or canvas - not appropriate for sharing on social media or public facing website)
- Waiting room (admit only those that you know, preferably via registration)
- Require authentication to join (when all attendees have University of Sussex accounts)



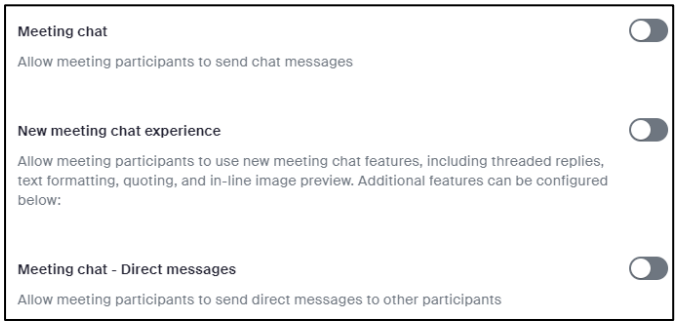
- Keep host and participant video off.



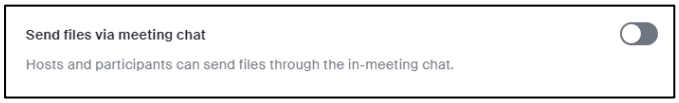
- Do not allow participants to join the session before the host.



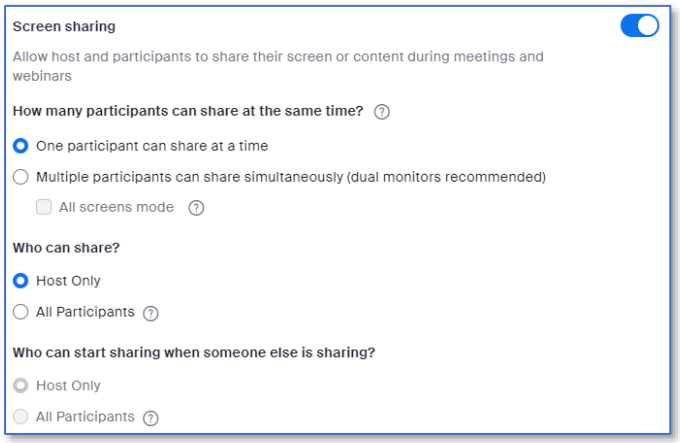
- Generate a meeting ID for each new meeting. Do not use your Personal Meeting ID.



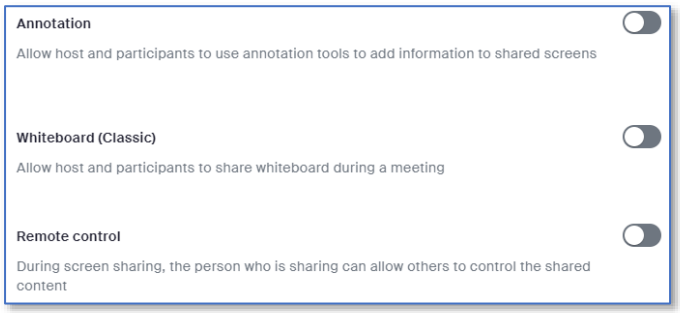
- Disable meeting chat.
  You can reinstate this within/during the event if you wish.



- Disable the ability to send files within the chat.



- Set screen-sharing so that only the host (and co-hosts if relevant) can share.

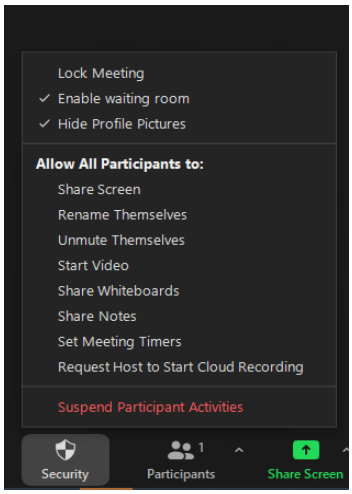


- Keep annotation, whiteboard and remote control switched off. This can be changed during the event if needed/desired.

In-meeting Security

Check the in-meeting security settings by clicking on the green shield icon in the top left corner.

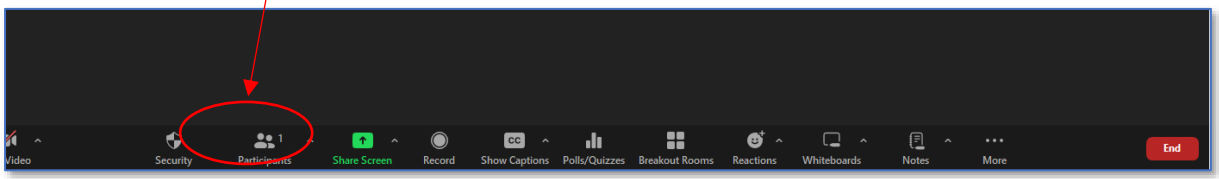
Familiarise yourself with the security settings on the bottom left of your toolbar and toggle on/off as needed.

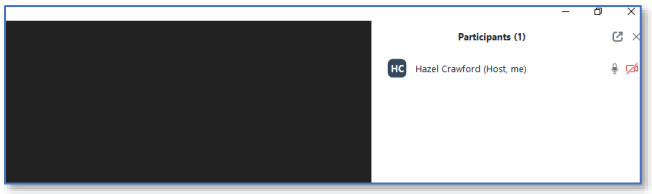


Note specifically the ability to:

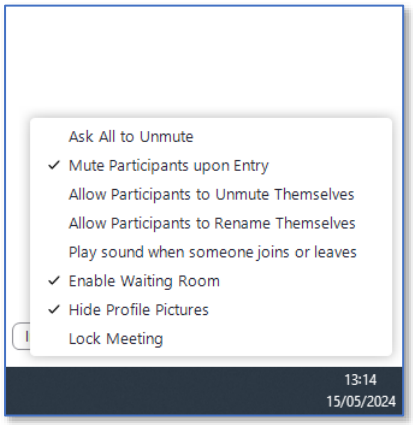
- Lock the meeting
  (ie. prevent new participants from joining)
- Hide profile pictures
- Enable a waiting room
- Suspend participant activities
  (ie. turn off *all* participants' video, audio and ability to share screen)

Click on the 'Participants' tab at the bottom of your screen to view all participants in a pane on the right.



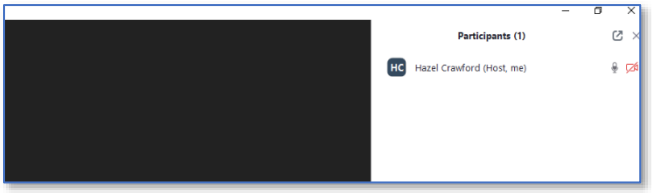


Note at the bottom of the pane the ability to “Mute All”.



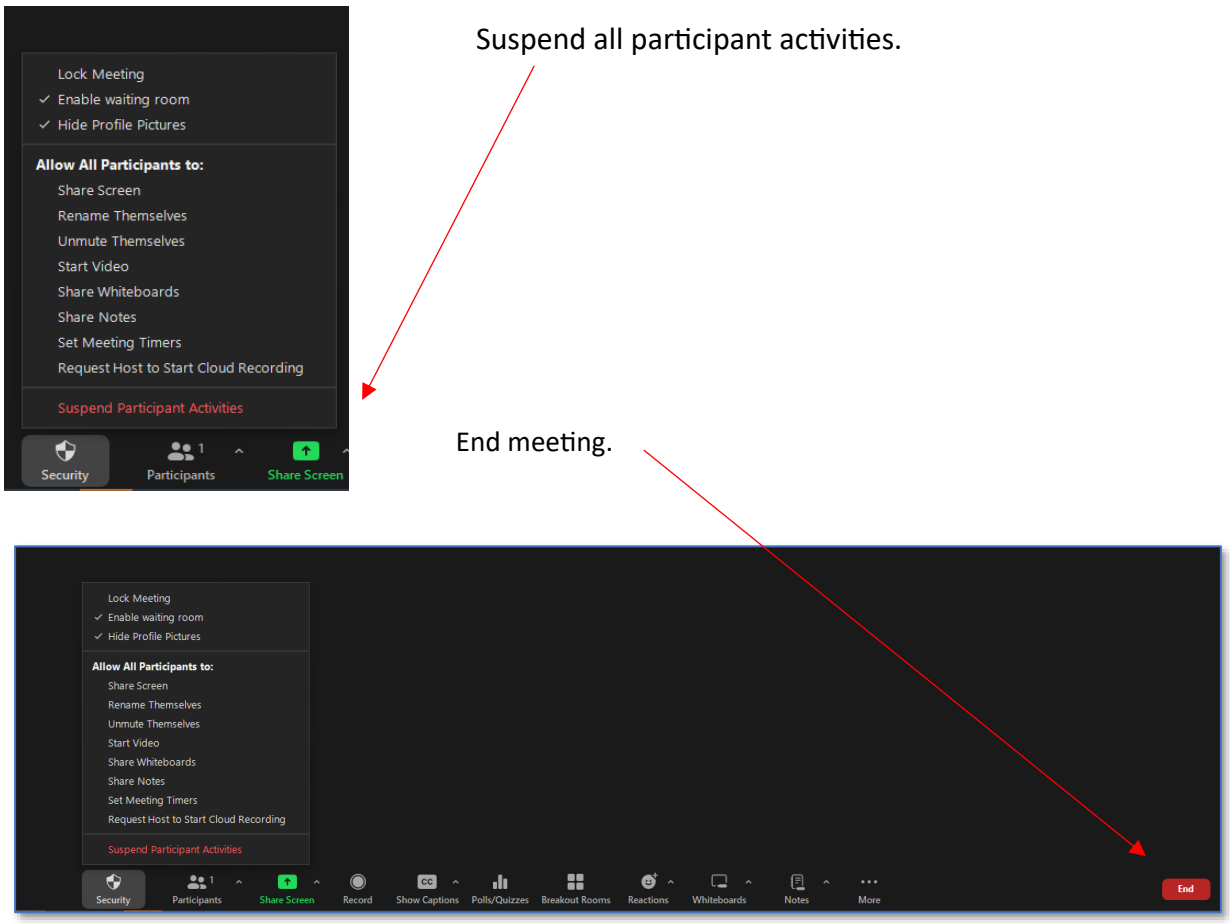
Clicking on the three dots at the bottom right of your screen enables you to control the mute settings, amongst other things.

Dealing with a Security Breach



To remove someone from the meeting, hover over their name and select “Remove”. By default, someone who has been removed cannot rejoin.

If you have made a mistake and removed someone by accident or the wrong person, go to the Zoom web portal and locate: Settings > Meeting > In-Meeting (Basic). Toggle on the setting called “Allow removed participants to rejoin”.



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.

Reporting Incidents of "Cyber-Bombing"

Any incidents of cyber-bombing on Zoom should be reported to ITS.

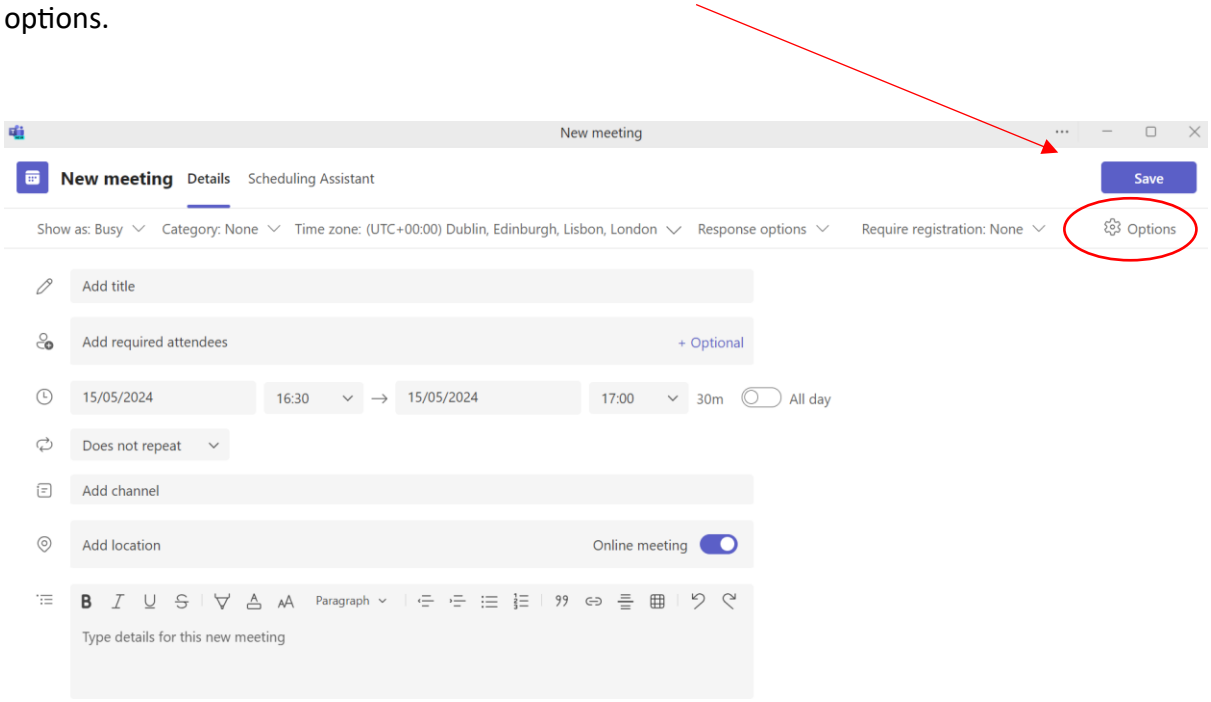
And also to Zoom.

Teams Security

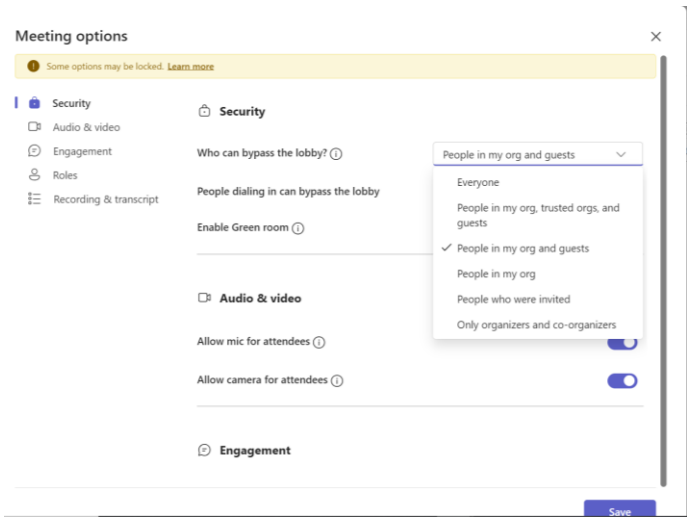
As with Zoom links, It is not recommended you share links to Teams-based meetings/events via social media - either directly within a post or on a registration form (e.g. Ticket Tailor, Eventbrite, Microsoft Forms, Google Forms etc.). Instead, meeting attendees should be provided with the link close to the date of the event when hosts have had the chance to check registrants' details.

Much of the advice detailed above in relation to Zoom security also applies to Teams.

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

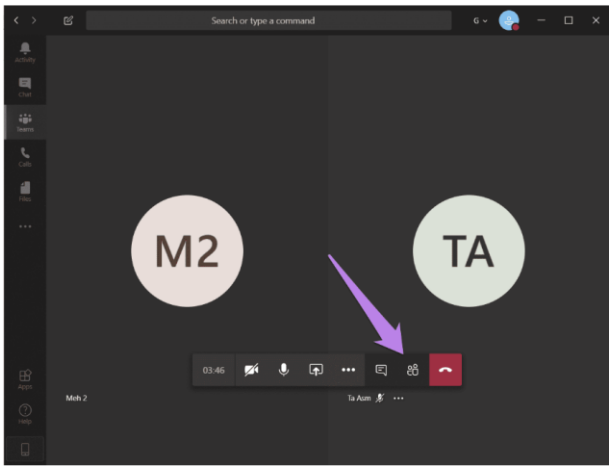


Click ‘More Options’ to access the full choice of settings.

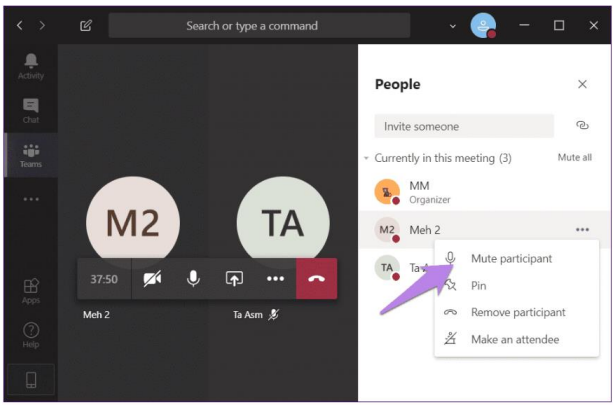


These include:

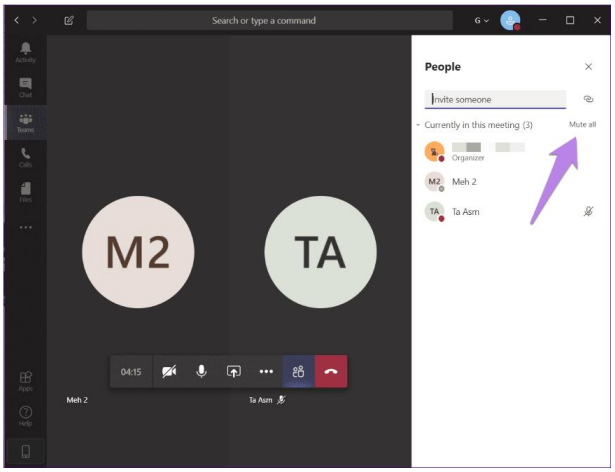
- Creating a waiting room - and any specified individuals who can bypass it if necessary.
- Allowing mic and camera for attendees.
- Meeting Chat: Toggle on or off to enable this function for attendees.
- Setting co-hosts.
- Choosing who can present.
- Recording and transcription.



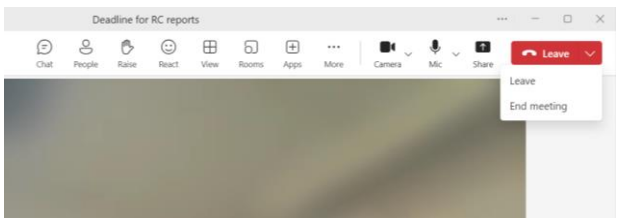
To view the list of participants, click on the Participants icon at the bottom of the screen.



To mute or remove a participant, hover over their name, click on the three-dot icon, and select the relevant option.



How to “Mute All”.



To end a Teams meeting, click on the red button in the top right. The downward arrow to the right gives you the option to end the meeting for all.

Any incidents of cyber-bombing on Teams should be reported to ITS.

Further Sources of Advice and Guidance

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 ITS at Sussex

Microsoft Teams support page from ITS at Sussex