ZOOM SECURITY AND BEST PRACTICE

What security should I apply to my Zoom meetings?

For all Zoom meetings we recommend:

- Using a **meeting password** or **enable waiting rooms**
- **Scheduling meetings using unique meeting IDs;** only use your **Personal meeting ID (PMI)** for one-to-one meetings.
- **Set screen sharing to 'Host only'** (you can override this in-meeting via the Share Screen settings).

For one-to-one or small meetings (up to 12 participants)

- Set a **password**
- Consider **locking** the meeting once in progress

Medium meetings (up to 30 participants)

- Set a **password**
- Make calendar invites **private** or send the password separately
- Consider using a **waiting room**
- Restrict screen sharing to **Host Only**
- Consider **locking** the meeting once in progress

Large meetings (30+ participants)

- Set a **password**
- Restrict screen sharing to **Host Only**
- Consider enabling **authenticated users** to restrict participants to **Zoom account holders only** or **Newcastle University staff/students only.**
- Enlist a colleague to help **manage participants** and **monitor chat**

Teaching sessions or webinars (where the content delivery is predominantly one-way)

- **Set a password**
- Consider using **waiting rooms**
- Restrict screen sharing to **Host Only**
- Schedule the meeting for participants to join with both their **audio and video muted**
- Advise participants to interact via the **Zoom chat**
- Enlist a colleague to help **manage participants** and **monitor chat**

Note: You can easily **remove a participant** from your meeting via the participant list. Once removed, the participant **will not** be able to re-join.