CYBER SAFETY

KEEP DEBATES PRIVATE

It is important to ensure that debates are private.

- In Zoom, meeting passwords help prevent unwanted participants from joining your meetings and inappropriately eavesdrop on discussions. Participants will be asked for the password before they can join the meeting.
- Please keep the meeting IDs private, only releasing them to students who are directly involved in debates.

MANAGE MEETINGS

The DAV staff will keep meetings safe by:

- Managing participants through the use of a waiting room or removing unwanted attendees.
- Locking a meeting room after it has started to prevent unwanted participants from joining.
- Moderating meetings and participants including muting and controlling screen sharing.

STAY ALERT FOR SCAMS

Watch out for fake or scam phishing messages/invites which can be used for identity theft or to access your account.

- Be alert for suspicious messages/invites including links appearing from unknown or unexpected meetings or senders.
- All DAV-based Zoom links will start with https://us02web.zoom.us/.
- Where possible join Zoom meetings via your calendar or the Zoom application.

BE RESPONSIBLE WHEN USING RECORDING

If you need to use the meeting recording features, apply a responsible approach by:

- Ensuring all meeting participants are aware that recording is being used (e.g. verbally announce this at the start of the meeting).
- Participants will be able to see a “Recording” visual indicator in Zoom meetings.
- Being aware that when recording a meeting any chat, video or audio content may be recorded.
- **As per the Rules for DAV competitions, no other recordings of debates are permitted without prior permission.**

KEEP APPLICATIONS UPDATED

Keeping your conferencing application updated to the latest version means that you will receive any important enhancements to maintain security.