CHECKLIST FOR VIDEO CONFERENCING (FOR COMPLIANCE)

USE OF ZOOM

A - ACTIVATE

1. **Correct Settings (Before Class)**

   - **Enable**
       i. **Use Unique ID** for meeting or only allow access by email address only
       ii. **Enable password** for the meeting, **use a strong password**
       iii. **Enable a Waiting Room** - participant will have to be admitted to the meeting (if available)
       iv. **Enable Mute all participants**

   - **Disable**
       i. **Disable file sharing** to avoid sharing of malicious files
       ii. **Disable all remote control and remote support** feature what will allow users to take over your device
       iii. **Disallow participants to join before host**
       iv. **Disable recording** unless required (note that students/participants may still be able to take a recording of the session using other recording tools)
       v. **Disable screen sharing for all participants**
       vi. **Disable annotation/whiteboard for all participants**
       vii. **Disable private chat**

2. **Meeting Schedule**
   - **Post the meeting details in an SLS lesson.**
       i. **Do not post the meeting details on publicly accessible platforms** such as the school's website or Facebook.
       ii. **Restrict the dissemination of the meeting details** to only the participants.

3. **Establish Rules for Your Students**
   - Do not share the meeting details with others
   - Use your real name to log in, not a pseudonym, e.g. Index Number + Full Name
   - Wait for your teacher to verify you and your classmates
   - Switch on your camera to allow your teacher to identify you
   - Observe cyber wellness, e.g. respect others by using appropriate language and not sending inappropriate content to your peers

B - BEGINNING THE LIVE LESSON

   - **Be early for the meeting and check through the settings**
   - **Verify your students** (both by name and face) **INDIVIDUALLY**
       i. Do not allow all your students to enter all at once.
       ii. If there are unidentifiable participants, do not admit them.
       iii. If student used a different name, ask them to change to their real name before admitting them.
   - **Lock your meeting room**

C - CONTROLLING THE SESSION

   - **Start your lesson and ask your students to switch on their camera views**
   - **Conduct your 'live' lessons while monitoring the students** like you would in a classroom

D – DEFEND

If intruders enter your class:

- Inform participants that you are ending the meeting and end the meeting immediately
- Adjust the necessary settings (see para 1 above) to prevent intruders
- Invite the participants to join the new meeting
- Verify that the intruder did not join the new meeting
- Lock the meeting room
- Explain to the participants what happened
- Identify any participants who have been emotionally affected by the incident
- End the meeting, counsel or refer the affected participants to a school counsellor (if necessary)

If students abuse the platform:

- If the intruder is a student from another class, or if your students abuse the platform, please report the incident to your discipline committee for their follow-up actions.
- If the intruder is unidentified or unknown, inform your HOD ICT and School Leader IMMEDIATELY of the incident and provide the following details:
    - Date and time of the incident
    - Name and contact information of the staff involved
    - Application used and on what type of device
    - Details of the unwanted guest and actions done (e.g., username, and screenshots of the incident if any).
- Please also report any incidents to MOE ITD at MOE_ITD_COMMS@moe.gov.sg