VIDEO CONFERENCING:
Guidelines to Keep You and Your Students Safe

TIP 1:
ONLY USE SCHOOL / DISTRICT-APPROVED TOOLS

1. **Do not host school business via unapproved tools.** Use only tools that have been provided or approved by your school or district.

2. **Carefully review meeting invitations.** Be wary of links sent by unfamiliar addresses.

TIP 2:
SECURE YOUR MEETING FOR ATTENDEES

1. **Only make meetings “public”** when necessary for the planned audience.

2. **Have a plan to terminate a meeting** if needed.

3. **Require a meeting password** and use features such as a waiting room to secure private meetings.

4. **Provide a link to the meeting directly to your students** and share passwords in a separate email.

TIP 3:
SECURE YOUR STUDENT OR SCHOOL’S INFORMATION

1. **Manage screensharing, recording, and file sharing options.**

2. **Protect sensitive information** especially when screensharing and displaying school information.

TIP 4:
SECURE YOURSELF AND YOUR STUDENTS

1. **Don’t reveal information unintentionally.** Check your visual and audio surroundings to safeguard personal information.

2. **Consider your surroundings.** Move, mute, or disable virtual assistants and home security cameras.

3. **Check and update your home network.** Change default settings and use complex passwords for your Wi-Fi network.

05/13/2020

For more information, visit cisa.gov/telework and schoolsafety.gov.