



Jon J.P. Fernandez
Superintendent of Education

Guam Department of Education
Curriculum and Instructional Improvement
Office of the Deputy Superintendent
501 Mariner Avenue, Barrigada, Guam 96913
Telephone: (671) 300-1635/1247
ciioffice@gdoe.net



Joseph L.M. Sanchez
Deputy Superintendent,
Curriculum and Instructional Improvement

VIDEO CONFERENCING GUIDANCE FOR SCHOOLS, TEACHERS, STUDENTS, and FAMILIES

Updated 9/22/20

The following guidance is provided to schools, teachers, students, and families on the use of Video Conferencing for class sessions, meetings, workshops or events.

A. Teacher-Parent/Guardian-Student Agreement

- a. All school employees are subject to **Board Policy No. 379: Education Technology Use**, in and out of school when communicating with students and parents/guardians.
 - i. **IMPORTANT NOTE:** BP379 was written and adopted during pre-COVID times and is consequently missing a number of key points that need to be directly addressed and clarified considering the focus on Distance Learning and the accompanying high volume of online work being conducted by personnel both in and out of school. While the policy is being reviewed and revised, please take note of the following points to support and clarify its overall intent:
 1. The GDOE network is referring to the GDOE internet system at the schools and central offices. When employees are connected to the GDOE network, it means their devices are connected to the Wi-Fi network and accessing the Wi-Fi signal that is within our facilities and NOT their personal home network.
 2. Though their home networks are NOT considered part of the GDOE network, when conducting GDOE business such as email, video conferences, etc., all employees' actions and conduct still fall within GDOE policy, most especially when interacting with students and parents. It does not matter if they are using a personal or GDOE device. Whenever conducting GDOE business, the policies regarding conduct still apply.
 3. However, this DOES NOT mean that GDOE can access the content of your personal computers/devices at home or even when connected to the GDOE network. The content of your personal computer/device is private and will not be accessed by any GDOE personnel. GDOE does not have the right or even the ability to access the content of your personal computers/devices, even if you are connected to the GDOE Network.

4. Though the content of personal computers/devices are private, when connected to the GDOE network, employees' web traffic is digitally monitored, specifically, websites visited. This is a requirement as the funding for our online access has strict guidelines governing its use for educational administration and curricular purposes.
 5. Regarding GDOE laptops/devices issued to employees- this is what the policy was specifically meant to address. The content of any GDOE employee's department issued laptop/device is NOT private and can be accessed by authorized GDOE personnel as needed. This is the same as your GDOE email addresses and google drive files. GDOE equipment are meant to conduct GDOE business regardless of the networks they are connected to.
- b. Teachers must ensure that all parents/guardians complete the "Education Technology Use Policy Parent/Guardian Agreement" found in the appendix of Board Policy 379: Education Technology Use. This agreement must be completed and submitted to the school/teacher by the parent/guardian and kept on file for the duration of the child's enrollment at that school. This agreement must be renewed at each new school the child enrolls in. Electronic submissions or confirmation of approval via email or phone are allowed and encouraged during school closures. This confirmation must include the name of the parent/guardian, the school employee documenting the confirmation, and the date/time.
 - c. Teachers may record video sessions with students only after parents have signed and submitted the Media Release Authorization Form. Electronic submissions or confirmation of approval via email or phone are allowed and encouraged during school closures. This confirmation must include the name of the parent/guardian, the school employee documenting the confirmation, and the date/time. Students (parents/guardians) who do not wish to participate in the recorded portion of a Video Conference will be excused for this portion of the session.

B. Family Educational Rights and Privacy Act

The Department shall ensure that the Family Educational Rights and Privacy Act (FERPA) is met when using video conferencing for instruction. FERPA is the federal law that protects the privacy of Personally Identifiable Information (PII) in students' education records. "Education records" are those records that are: (1) directly related to a student; and (2) maintained by an educational agency or institution or by a party acting for the agency or institution. For more information related to FERPA and virtual learning, refer to the March 2020 resources on *FERPA and Virtual Learning*: <https://studentprivacy.ed.gov/resources>.

C. Video Conferencing & Circumstances beyond the control of the school or the teacher

Video Conferencing is an essential part of participating in an online class. It often encompasses the main instructional part of the class and allows for students in the class to interact visually with each

other and the teacher. Unfortunately, like many online strategies and activities, there are certain risks that come with participation. Even with strict rules and expectations, many of these risks are unavoidable and therefore students and their parents/guardians need to be aware of these risks and understand what they mean before participating or allowing their child(ren) to participate in a Video Conference. Please take note of the following:

- a.** Parents/Guardians need to understand that Video Conferencing involves their child(ren)'s image and voice being digitally transmitted over the internet to the computer screens of other participants,
- b.** Parents/Guardians need to understand that there are a number of circumstances or conditions that are beyond the control of the school or the teacher including:
 - i.** Who is with the other participating children at home or near the computer/device a child is using and, therefore, who will hear or see what is on the computer/device screen,
 - ii.** What is in the background of another child(ren)'s camera view,
 - iii.** What other children, their parents, or other individuals say or do on the microphone or camera, or,
 - iv.** Other children, their parents, or other individuals taking a picture of the computer screen or recording the audio during a conference using an external device such as a phone or camera.
- c.** Parents/guardians need to understand that the Video Conferencing application Google Meet is an open platform similar to WhatsApp, Facebook, Instagram or any other social media platform that is available to the public and, in particular, to anyone with a Gmail account. This means individuals, including students, are able to generate their own Video Conference sessions without the need for a teacher's approval.

Additionally, students can engage in a Video Conference before the teacher arrives to the session, after the teacher leaves a session, and independently without a teacher by generating their own VC link. In these cases, students are considered to be engaging in an unsanctioned online activity and thus will not be the responsibility of the school or the teacher during these times. Parents/guardians are responsible for ensuring that their child(ren) are engaging in approved online activities.

- d.** Teachers must ensure that all parents and students understand these risks associated with these circumstance and conditions before participating in a Video Conference. Once this information is provided, subsequent participation in a Video Conference means that the parents/guardians are aware of these circumstances and conditions and are knowingly consenting for their child(ren)'s participation.

D. Expectation for students during Video Conferences

- a.** Each school and teacher may provide additional and specific expectations, however, all students must adhere to these minimum expectations when participating in any Video Conference sponsored by their teacher, school or the district.
- b.** Video Conferences are considered official school/class time and students must act accordingly.
- c.** Students should be dressed appropriately in a manner that is comfortable but at the same time presentable in public.
- d.** Students will follow all teacher instructions regarding class activities and camera/microphone settings including, but not limited to, when to turn cameras and microphones on or off, when to share or write on screens, and when to post comments or provide responses either visually, verbally, or digitally.
- e.** Students will be engaged throughout the Video Conference session by actively listening to presentations and speakers, watching the video monitor, taking notes, asking/answering questions and participating in class discussions.
- f.** Inappropriate or unwelcomed behaviors, actions or comments by students or any other individual accompanying a participating student may result in disciplinary action, which may include immediate removal from the Video Conferencing session.

E. Expectations for parents/guardians during Video Conferences

- a.** Parents/guardians shall make every effort to ensure that no one other than the student scheduled for the class and their parents/guardians can see or hear the Video Conferencing session.
- b.** Parents/guardians shall make every effort to ensure that the students participating in the Video Conferencing session will be protected from seeing or hearing any inappropriate content in the background or the surroundings coming from your household.
- c.** No video or audio recordings of any Video Conferencing session shall be made by the parents, guardians or students without the expressed permission from the teacher.
- d.** If parental/guardian or other third-party assistance is needed for a participating student during a Video Conferencing session, the individual assisting the student shall not disclose any personal identifiable information about any student participating in the class. Specific actions or comments made by students during a class are considered confidential and should not be discussed or shared with anyone outside of those participating in the Video Conference.

- e. Parents/guardians are responsible for the actions and words of anyone accompanying their child(ren) during a Video Conference session. Inappropriate or unwelcomed behaviors, actions or comments by any individual accompanying a participating student may result in disciplinary action, which may include immediate removal from the Video Conferencing session.

F. Professional Practices

- a. Teachers must have established ground rules and expectations for all virtual sessions.
- b. Teachers should be dressed professionally when on video sessions with students.
- c. Teachers will handle student misconduct on video sessions in the same manner done in traditional learning settings; they will provide progressive interventions for students' inappropriate behaviors.
- d. All school employees are legally obligated to report suspected child abuse or neglect.
- e. The three Models of Learning reinforce a viable, equitable instruction for all students.

G. Video Recordings

- a. Teachers should conduct video sessions with their video on and, if possible, in a designated space that is free from distractions.
- b. Teachers are to announce that the session will be recorded prior to the beginning of the session.
- c. Video recordings of live sessions should only be done if they are in direct relation to the lessons. Rights to these recordings should only be shared through the GDOE Google drive with students given "**view**" access only.

H. Virtual Platforms, security settings and best practices for online safety

- a. Teachers must use the GDOE's accepted online platforms: Google Classroom, Moodle, Zoom, Google Meet and any other approved or accompanying online tools in the G-suite for education to conduct their lessons.
- b. **Google Meet is the Video Conferencing platform currently available** to all teachers and students. When utilizing Google Meet, please take note of the following security settings and best practices for online safety:

1. When you commence your Google Meet, click on the three vertical dots located on the bottom right of your screen (computer) on most mobile devices the vertical three dots are located on the top right of your mobile device screen.
2. You will see several menu items and click on “Settings” which enables you to set your video and audio settings.
3. Teachers can create nicknamed meetings to prevent students from re-using class meetings This will prevent students from rejoining a meeting after it has ended. Teachers can reuse the same nickname, but students will not be able to join until the teacher is present and will not be able to rejoin once the last person has left. To create a nicknamed meeting, use one of the following methods:
 - a. Use a short link like g.co/meet/nickname
 - b. Go to meet.google.com or the meet mobile apps and enter a meeting nickname in the “join or start meeting” field.
 - c. Use the meet code automatically generated by Google Classroom.
(<https://support.google.com/a/answer/9822731?hl=en>)
4. The Record Meeting is secure in terms of the following:
You can record if:
You’re the meeting organizer
You’re in the same organization as the organizer
You’re a teacher signed in to your G Suite account, but not a student

c. **Zoom is another Video Conferencing platform** used by the GDOE and a number of GDOE teachers. The department is currently working on obtaining a zoom account for all teachers, as we would like to increase the security of our Video Conferences and improve their overall management. For those teachers currently using zoom, please take note of the following security settings and best practices for online safety:

1. On your URL type in zoom.us
2. Log into your account using your login credentials Suggestion to “sign into Zoom is type into GDOE e-mail address and simply click “Sign in with Google”
3. Click on “*My Account*” on the top right corner of your screen
4. Within your profile click on “*Settings*” on the left side of your screen
5. Within Settings you’re able to configure security settings which will keep you and your students safer.

MINIMAL SECURITY SETTINGS:

1. *Do not allow “join before host”*
 - a. Similar to your classroom. Teachers have an option to have students wait before entering the room. (optional), if you would like to allow students to join before host, you can enable a waiting room to have them enter.
2. *Enable “waiting room”*
 - a. This will allow teachers to screen entrants prior to entering the Zoom Classroom. This is completed by clicking on the button on the right side of your screen you’ll see Modified or Reset on the right side of the button.
 - b. You can customize what your waiting room looks like by clicking “Customize Waiting Room”. You can add a disclaimer to alert students and

individuals that this is an official DOE classroom and only approved students will be able to enter the classroom.

3. *“Require a passcode when scheduling new meetings”*
 - a. Enable this setting to allow only those who you have given your password to enter the waiting room or Zoom meeting.
4. Other suggestions: Limit screen sharing ability (default); disable participants to record (default).

ADVANCED SECURITY SETTINGS:

5. “Lock Session”
 - a. As soon as you have all your students, teachers can “lock the room”. In the meeting, the host can click participants at the bottom of the Zoom window and click “Lock Meeting.” This will restrict any further entrants from coming into the room.
6. Allow only Authenticated users
 - a. Teachers can restrict entrants to only participants with specified e-mail domain or participants that have Zoom accounts. Click on “Only Authenticated users can join meetings.” NOTE: Signing into Zoom is the default, but you can edit this and require possible attendees to sign into GDOE domain account. *Caution: You must send personal invites to attendees when you select this option. See: <http://bit.ly/authenticatingprofiles> for detailed information.*

End...