Practices for Keeping Members of our Archdiocesan School Communities Safe while Online for Distance Learning

The following recommendations should be implemented by schools, students, and families in Archdiocese of Denver Catholic Schools.

Teacher Actions

- Teachers have a professional obligation to act with decorum and ensure a safe environment for all students. This applies whether it's an in-person setting or a virtual/audio setting.
- As a frame for thinking about keeping a safe environment during distance learning online, consider how we would approach student-teacher interactions in an in-person setting. We don't prohibit teachers from engaging one-on-one with students. There are precautions put in place (i.e. keep the door open, never put yourself in a potentially compromising situation). Virtual environments certainly add a level of complexity, but the same approach and precautions need to be kept in mind. Try to mimic the in-person precautions when online.
- Maintain professional appearance on camera.
- When teaching online synchronously, be in a common area in your home, ensuring your screen is visible to any roommates or family members.
- Share all links for synchronous class sessions with administrators. This allows administrators to pop-in without notice.
- Consider recording all synchronous classes. This is a measure of protection but can also help your administrator with performance evaluations.
- Use asynchronous (recorded) videos whenever possible. Always share links to the asynchronous class sessions with administrators.
- Share all links for synchronous and asynchronous class sessions with parents as well as students.
- Always allow parents to join synchronous class sessions. Teachers may ask parents to not participate, but certainly parents should be able to be present whenever they'd like.
- If one-on-one sessions are going to be requested for additional support/instruction, intervention or remediation, teachers should inform not only their principals, but also parents and let them know they're requesting a session and why they're requesting it. Overcommunication on this front is essential.
- Do not use social media to communicate directly with students one-on-one (e.g., Facebook Live, Instagram Live). Do not use personal social media to communicate with students whatsoever.
- Only use your school-approved communication platforms (e.g., Zoom, Google Classroom, school email)
- Any profiles displayed on sites should be reflective of the teachings of the Catholic church and uphold the virtues of the Catholic faith.

Teacher Actions (cont.)

- Particular notes for virtual meetings/synchronous classes:
    - Post links to synchronous classes or virtual meetings in a location accessible only by participants allowed to be in the session. Do not post links to synchronous class sessions on school social media pages.
    - For digital office hours, use a link that is open to all students and/or administrators and/or parents to join. This is equivalent to leaving your door open in a physical classroom.
    - Limit screensharing to teachers only.
    - Only used agreed-upon educational and school-approved platforms (such as Google Classroom, Google Meet, Microsoft Teams, etc.) to meet students online.
    - If posting images of virtual meetings on school social media, be sure to block student names and any join codes that could be visible in the picture.
    - Be sure to know how to remove any unwanted participants from the virtual learning session.
    - Specific notes regarding Zoom:
        - **Students should wait in the "waiting room" before entering class**. This helps the teacher control who is let into the Zoom, and ensures that no one is able to access the Zoom unless approved by the host (teacher). Waiting rooms need to be turned on in the host's account settings.
        - **Keep Zoom links private**. Don't share on your class website or any other publicly viewable site. Email or direct message Zoom links to families/students.
        - **Create a new personal meeting ID Zoom meeting if yours has been shared publicly**. Zoom allows you to use the same personal meeting ID for every meeting. If you have shared your meeting ID publicly in some way – perhaps on a non-password-protected site, contact Zoom to receive a new personal meeting ID.
        - **Require a Zoom meeting password.** Zoom will create a meeting password that will generate with the invitation to the Zoom that is sent over email or direct message to families. This makes the Zoom meeting more difficult for random participants to join.
        - **Control screen sharing to host only**. Zoom recently updated the default screen-sharing settings for education users to be "host-only" screen sharing. That said, please double check that only the host can screen share. This helps prevent students from sharing random content with the class. If you are using screen share as a check for understanding, the host should be able to lock others from sharing as much as possible on the Zoom.
        - **Lock all classrooms**. Once all students are in the Zoom, the host (teacher) should lock the classroom so no one else is able to join. Give students a few minutes to file in and then click Participants at the bottom of your Zoom window. In the Participants pop-up, click the button that says Lock Meeting. If your principal wants to pop in to classes, classes should not be locked.
        - **Control student ability to chat**. Teachers can restrict the in-class chat so students cannot privately message other students. We'd recommend controlling chat access in your in-meeting toolbar controls (rather than disabling it altogether) so students can still interact with the teacher as needed.

Student Actions

- Ensure that your screen can always be viewed by someone else.
- Complete your class sessions in common areas of the house.
- Make sure you have ability to contact a safe, trusted adult during your online sessions.
- Do not privately chat other students. Do not chat with teachers about anything besides academic work.
- Maintain appropriate dress when on synchronous learning sessions.
- If you see something in appropriate online, shut your computer right away, or put it face down. Walk away. Tell a trusted adult what happened.

Parent Actions

- Ensure that your home devices have web filters installed. See recommended resources for web filters below.
- Web filters are not always enough. Sometimes children will inadvertently see images on websites that are not suitable for children. Teach children explicitly what to do when they see these images: close their eyes, close the computer if possible, walk away, tell an adult what they saw and ask the adult to get rid of the image.
- Require students to only use technology in shared living spaces.
- Make sure you can always see your student's screen—you don't need to be looking at it every moment, but you should be able to glance over to see what is on your child's screen.

FERPA and Virtual Learning:

- What is an 'education record' under FERPA? "Education records are those that:
    - Directly relate to a student; and
    - Maintained by an educational agency of institution or by a party acting on behalf of the educational agency of institution.
- Video recordings of virtual classroom lessons qualify as "education records" protected under FERPA only if they directly relate to a student (i.e. contain personally identifiable information-PII) and are maintained by an educational institution.
    - If a student appears in the video recording of a classroom lesson, it is an education record.
- Schools should include instructions for students regarding not sharing or recording virtual class engagements, including screenshots of class/classmates, selfies, or personal video recordings.
- School personnel should not share video recordings, screenshots, selfies on social media or other public forum without consent of principal and consent of parents if it contains personally identifiable information.

FERPA and Virtual Learning (cont.):

- Assuming the video recording does not disclose personally identifiable information during a virtual classroom lesson or if written consent is obtained, FERPA would not prohibit the teacher from making a recording of the lesson available to students enrolled in the class.
- Questions to consider before posting video recordings:
    - Will the video recording be maintained as an education record, and is it directly related to a student?
    - What if any, personally identifiable information did the video recordings capture?
    - With whom is the school sharing the video recordings?
    - How is the school protecting from unauthorized disclosure of video recordings that qualify as education records or that contain personally identifiable information?

Recommended Web Filters

- Please see the following page for recommended web filters. We ask that all parents be informed of web filter options.

Web Filter Options for Families

Product Name	Costs	Installation	General Description Capabilities
Bark	Always free for schools	Very simple under the GSuite Admin and Office365 portals https://help.bark.us/en/articles/1673331-how-to-set-up-bark-for-schools-for-g-suite	• Has a web filter that is more robust than the traditional G Suite admin web filter due to the ability to block whole categories. Furthermore, the reporting feature is nice because it tells us who was blocked. https://help.bark.us/en/articles/2937990-set-up-chrome-web-filtering-bark-for-schools • Features an upgrade (paid edition) called "On Call", this service calls the admin and the parents to notify them when the student is in immediate danger. https://help.bark.us/en/articles/3676038-bark-oncall • Bark for Schools comes with a free Parent Portal as well. Furthermore, if the parents decide they would like to sign up for "Bark for Families", they get a 20% discount off of the normal price which is $9.99/mo or $99.99.
GoGuardian	Free until the end of this school year. I am still waiting for the quotes!	Admin Software installation to PC or MAC. This system requires Google Enterprise for Education. It has a friendly interface for admin to customize the monitoring policies besides its default internet firewall protection. It monitors Internet activities based on the device, not the user.	• There are four core products: GoGuardian Admin (web filtering), GoGuardian Teacher (classroom management), GoGuardian Fleet (chrome device management), and GoGuardian Beacon (Suicide and self harm alerting). • These services monitor student activity online, filter content, and alert school officials to possible suicidal or self-harm ideation. It is suitable for managing Chrome devices.

CovenantEyes		Most platforms except Chromebook. Promo code for 30-day trial: chasity.	• It's an internet accountability that doesn't block but monitors the internet activities of the entire family.
Securly	Free filtering and audit until end of school year June 2020. Willing to offer the "Full Solution" package for this time as well.	• Online meeting with IT reps from schools • IP Addresses • Compatible with all devices • Quick deployment and can be achieved within 1 or 2 days	• Google G Suites Enterprise EDU Option • Overarching focus is to support monitoring of student activity and instances of cyberbullying, suicide, etc.

Parent Options

- Call your internet provider to see what is available
- Free: Using the built in Parent Control for MacOS, Windows Family for Windows Devices, and Google Family Link for Chromebooks
- Nominal: MobiCip - protects up to 10 devices on any platform for $60.00 per year.
- Premium: Norton 360 w/ LifeLock Select protects up to 5 devices for $100 per year and includes credit monitoring, and so much more.

Known Challenges:

- Various devices used throughout the schools i.e. Chromebooks, iPads, laptop computers, smartphones, iPad mini's, etc.
- Various platforms are used by schools i.e. Google Suites, Microsoft 365 EDU
- Ownership of devices varies ie. school managed vs student owned devices
- Student database management may vary
- Student populations vary
- Various firewalls in place such as watch guard

Web Filter Recommendation Taskforce Members:

Name	School	School Role and Background
Roxanne Elsner	St. Mary Littleton	• Technology Teacher and technology Tier 1 Support • Retired JPMorgan Chase Ops Manager and Cash Services Hurricane Katrina Team member
Norris Davis	St. Mary Littleton	• Technology Resource and Network Admin and father of two students • Former network admin for Missouri school district
Erika Matteo	Notre Dame	• Media Specialist and technology teacher along with support for parish • Web design
Tuyet Nguyen	St. Therese	• Assistant Principal and technology resource, and network and system admin • Former employee at Dept of Defense
John Christopher	Assumption Catholic School/Parish	• IT Coordinator for school and parish, teaches technology and P.E. and father of four students • Former IT Director for Evergreen School