Directions for Maintaining a Safe Environment for Parish Religious Education: Grade Levels 1 through 8

September 2020 through May 2021

For the Weekly On-site Parish Religious Education Approach:

The Parish Program continues to carefully implement all the directives of the Archdiocesan Safe Environment Office established for the regular, weekly onsite Parish Religious Education Program.

The Parish Religious Education Program abides by all the state, area and local regulations regarding the Corona-19 Virus as well as all the directives issued by the Archdiocese of New York. These regulations should govern program sessions as well as all other meetings, gatherings and activities such as program registration, parent meetings, First Communion and Confirmation celebrations.

For the Family-Based Parish Religious Education Approach:

It is essential that all Parish Religious Education for children and youth (grade levels 1 through 8) be done through planning and communication with the parents not directly with the children/youth.

In using an online classroom setting such as ***Zoom*** or the ***Google Meet*** option in Google Classroom, just as in an onsite Religious Education setting, a Director, Coordinator or Catechist who is on the parish Safe Environment roster must always be the host. A co-host and/or guest presenter may also participate. In these live sessions, the parent /guardian must always be present with the child .

Directives for Safe Use of Zoom for Parish Religious Education: Grade Levels 1 through 8
(Used with permission of the Office for Catholic Schools, Archdiocese of New York)

In those cases in which a segment of Parish Religious Education is given to a group of children/ youth in a web-based classroom setting, the Safe Environment Zoom Directives established by the Office of Catholic Schools, Archdiocese of New York, should be followed. These directives as adapted to Religious Education are as follows.

An unwanted intruder is potentially dangerous, so it is critical that Directors, Coordinators and Catechists follow the recommended protocols to minimize the possibilities for outside interference.

Many of the security breaches in using Zoom have been the result of students sharing call access information on the internet and social media, not from Zoom's software being "hacked" or compromised. Relatively few "break ins" have been the result of a sophisticated hacker disabling

security mechanisms, although this is always a possibility with any internet platform. Most of the news-worthy issues with Zoom have been the result of hosts failing to secure the entry points to their Zoom sessions.

In using Zoom, Directors, Coordinators and Catechists providing Religious Education should follow follow these security guidelines:

1. Zoom's "Waiting Room" feature is the most important security feature the platform offers and must be activated. In fact, we recommend Zoom for student-facing live video because of its ability to regulate participants through use of a **Waiting Room.**

2. Require children/youth to enter a waiting room with a standardized display name (i.e. first Name and last name) to quickly identify unwanted participants requesting access. The adult hosts of the Zoom session should know the first and last names of all the invited participants.

3. Eliminate the option for children/youth to participate in the session by phone only. If this creates an issue of inaccessibility for some children, encourage the parents to provide access to Zoom video conferencing through the technological capabilities and willingness to share, of another trusted adult (friend, relative, parent in the religious education program)

4. Work directly with the parents to ensure that there is no sharing of call information by children/youth on social media. This has been the leading cause of Zoom sessions being interrupted. This is a serious security issue and any breach of it would necessitate discontinuing Zoom sessions.

5. Use the ***Critical Zoom Safe Environment Settings*** every time Zoom is used for a Parish Religious Education session or meeting. These settings are summarized below and the screen shots are attached.

6. Check regularly the Zoom settings to make sure they remain in accord with those listed below, and also be alert to communications from Zoom regarding changes made by Zoom itself.

Critical Zoom Safe Environment Settings: Settings are to be found at Zoom.us after log in.

+Computer Audio Only: Prevents unknown participants from joining via telephone
select Computer Audio and click on save

+Join Before Host Disabled: Prevents students from spending time in your "classroom" unattended. You become the first person in the call and regulate who enters with your permission.
Turn off Join before host

+Chat Enabled But Prevent Participants from Saving Chat: Allows all communication to be publicly visible and prevents students from obtaining a mutable "transcript" of the chat on their own device.
Turn on Chat
Then click on button for Prevent participants from saving chat

+Private Chat Disabled: Prevents students from messaging each other without teacher visibility.
Turn off Private Chat

+Play Sound When Participants Join or Leave Enabled (Host Only): Provides the host a small cue that someone has entered. This is particularly useful in preventing intruders if you are notified of someone joining the session at an unorthodox time, or if your whole class is already in the session.

Turn on Play sound when participants join or leave
Then click on button for Heard by host only

+Allow Host to Put Attendee on Hold Enabled: Provides a crucial security measure should you need to remove a participant and put them back in the "Waiting Room"

Turn on Allow host to put attendee on hold

+Screen Sharing Enabled (Host Only): Prevents students or unwanted participants from drawing text or symbols for all participants to see, or from showing inappropriate content. The host of the call retains sole control of screen sharing.

Turn on Screen sharing.
Then click on button that says Host Only

+Disable Desktop/Screen Share for Users On: Allows added security for screen sharing.

Turn on Disable Desktop/screen share for users

+Annotation Off: Prevents participants from marking up the shared screen. Note that this feature might be scaffolded in as the teacher and students gain comfort and trust on the platform

Turn off Annotation

+**Whiteboard On:** Allows teacher to present drawings for students to see, but not to add to.

Turn on Whiteboard
then click on button for Auto save whiteboard content when sharing is stopped.

+ Nonverbal Feedback On: Allows important engagement features for students to indicate whether they are following along by answering yes or no, raising their hand, or giving a thumbs up.

Turn on Nonverbal Feedback

+Allow Removed Participants to Rejoin Off: As a maximum security feature, once a participant has been removed from the meeting, they cannot rejoin. Teachers should communicate explicitly to students in violation of any Safe Environment policies that they cannot rejoin if they are removed.

Turn off Allow removed participants to rejoin

+Virtual Background On: Allows students to use a safe image for their background if desired.

Turn on Virtual Background

+Waiting Room On: No security feature is more important than enabling the Waiting Room as it allows the host of the session to regulate who can enter the session. Most of the instances of "Zoom Bombing"

have been the result of the Waiting Room being turned off and the teacher not maintaining control of who enters their classroom.

Turn on Waiting Room