ALGONQUIN COLLEGE | Cyber Security Unit

ZOOM Security and Privacy Guidelines

For Events Open to the Public

Version 1.1

1.0 PURPOSE OF THIS GUIDE

This document outlines the security and privacy safeguards that Algonquin College faculty and staff must implement to prevent and respond to Zoombombing when using Zoom-meeting for conducting events open to the public.

Zoombombing refers to the unwanted, disruptive behaviour of a participant(s) into a video conference call.

In a typical Zoombombing incident, a teleconferencing session is hijacked by participants engaging in behaviours that are lewd, obscene, racist, homophobic, offensive in nature or otherwise inappropriate, typically resulting in the shutdown of the session. This may include, but is not limited to, disrespectful gestures or body language, insults, display or sharing of offensive audio or visual material, inappropriate communication via chat, including sharing of malicious links or files.

Events open to the public involving a large audience are the preferred target of Zoom bombers. Where feasible and appropriate, these events should be conducted in a webinar format. If you plan to hold these events in a meeting format, follow these guidelines.

The following settings have been chosen to strike a balance between security and audience engagement and will protect video conference calls from most instances of potential Zoombombing.

2.0 PRE-MEETING SAFEGUARDS

1. Create a Zoom account and keep the app updated
   - Use only your Algonquin College email address
   - Create a strong password, using a minimum of 12 characters, with at least one upper and one lower-case letter, one number and one special character. You must not use the same password as an existing one
   - If you already have an account, go to the settings page and follow the next steps
   - Update ZOOM to the latest version
     If you don't update ZOOM, some of the features mentioned in this document may not be available (if you're having difficulties updating Zoom, check this tutorial)

2. Prevent any disruptions during your event
   - Settings → "*Meeting*" tab → "*Security*" → enable "*Waiting room*" → "*Waiting Room Options*" → Click "*Edit Options*" → Check radio button "*Everyone*"

- Settings → "*Meeting*" tab → "*Schedule Meeting* "→ enable "*Mute all participants when they join a meeting*"
- Settings → "*Meeting*" tab → "*In Meeting (Basic)*" → disable "*Private Chat*"
- Settings → "*Meeting*" tab → "*In Meeting (Basic)*" → disable "*File Transfer*"
- Settings → "*Meeting*" tab → "*In Meeting (Basic)*" → enable "*Screen Sharing*" and select the option "Host-Only"
- Settings → "*Meeting*" tab → "*In Meeting (Basic)*" → disable "*Annotation*"
- Settings → "*Meeting*" tab → "*In Meeting (Advanced)*" → disable "*Virtual Background*"
- Settings → "*Meeting*" tab → "*In Meeting (Advanced)*" → enable "*Report to Zoom*"

3. Disable automatic recording
   - Settings → "*Recording*" tab → Disable "*Automatic Recording*"

4. Do not allow participants to record the session
   - Settings→ "Recording" tab→ "*Local recording*" → Disable "*Allow hosts and participants to record the meeting to a local file*"

5. Ensure the privacy of participants joining the session by phone
   - Settings → "*Telephone*" tab → enable "*Mask phone number in the participant list*"

3.0 IN-MEETING SAFEGUARDS

It is highly recommended to implement these safeguards in the order below.

1. Add a co-host

   While presenting, it may prove difficult to monitor for, and react to, signs of disruptive behaviour and manage inquiries from the audience. By adding a co-host, you can focus on your presentation while assigning the task to monitor the participants to a colleague.
   - Once you start the meeting, admit only the colleague that you want to add as a co-host → Hover over your colleague's video → Click the more icon "…" → Click "*Make Co-Host*"

2. Post your house-keeping rules in the chat
   - Explain that all microphones are disabled by default. If participants have any questions they can: 1) submit them directly to the host; 2) raise their hands or request to the host via chat to speak and the host will unmute them

3. Direct all questions to you and prevent participants from posting publicly in the chat
   - Click on the three dots in the chat window and select *"Participant Can Chat With Host-Only"*)

4. Do not allow participants to unmute themselves
   - Click on the security button and uncheck "Allow participants to unmute themselves"

5. Admit all participants and disable the waiting room
   In the Zoom toolbar:
   - Click on "*Participants*" → hover the mouse pointer over the participants' names and select "*Admit All*".
   - Click on "*Security*" → Uncheck "*Enable Waiting Room*".

6. Do not click on any links submitted by participants in the chat

7. Do not record the session unless it is necessary to do so for a legitimate purpose. If you decide to record the session, you must inform participants and follow the procedure in section 5 of this document.

4.0 HOW TO RESPOND TO ZOOMBOMBING

Even if you implemented the precautions above, during large events there is always the chance of participants engaging in inappropriate behaviour.

Here are a few ways to respond to a participant disrupting your session.

1. Mute the participant
   - In the toolbar, click on "*Participants*" → hover the mouse pointer over the participant's name and select "*Mute*".
     If you previously haven't disabled "*Allow Participants to Unmute themselves*" and there are several people who are unmuted, it may be difficult to quickly identify which participant is the cause of the disruption. In this case, the quickest response is to mute all participants. You can do so by clicking the "Mute All" button in the Participants sidebar. Once you do this, you should also disable "*Allow Participants to Unmute Themselves*" as noted above.

2. Turn off the video of the participant
   - In the toolbar, click on "*Participants*" → hover the mouse pointer over the participant's name → click on "*More*" → select "*Stop Video"*

3. Remove the participant from the session
   - In the toolbar, click on "*Participants*" → hover the mouse pointer over the participant's name → click on "*More*" → select "*Remove"*

4. Report the participant to Zoom
   - In the toolbar, click on "*Security*" → Select "*Report*"
   - Select the name of the participant you would like to report
   - Check the reason for reporting this participant
   - Add any comments or screenshots providing evidence of the inappropriate behaviour

- This report is automatically sent to the Zoom Trust and Safety team to evaluate any misuse of the platform and block a user if necessary

5.0 HOW TO RECORD YOUR EVENT

The following safeguards **must be implemented by faculty and staff** before recording an event.

1. Inform the participants before recording by posting the following statement in the meeting chat so that it is available for the entire session:

   Please note that this session is being recorded for the purpose of ***(host to insert purpose here and specify whether the recording will be shared online on the College's website, social media, YouTube or other publicly available platforms)****. Personal information, such as video and audio recordings, collected through Zoom will be used by Algonquin College under the authority of the Ontario Colleges of Applied Arts and Technology Act, 2002, section 2 and in accordance with sections 39, 41 and 42 of Ontario's Freedom of Information and Protection of Privacy Act.*

   At Algonquin College we respect your privacy: if you wish to not be recorded, please leave your camera and audio turned off.

   If you have any questions about the processing of personal information by Algonquin College, please contact the Freedom of Information Coordinator, by phone at 613-727-4723 ext. 6407 or by e-mail via FOIcoordinator@algonquincollege.com

2. **Disable Participants' Video** and enable **Mute Participants Upon entry** to avoid any inadvertent collection of video or audio recordings from participants who don't want to be recorded **(one-time setup)**
   - Settings → "*Schedule Meeting* "→ uncheck the box "*Participants Video*" and check the box "*Mute Participants Upon Entry*"

3. **Disable Display Participants' name in the recording**
   - Settings →"*Recording*" tab →"*Cloud Recording*"→ uncheck the box "*Display participants' names in the recording*"

4. **Set a passcode to protect recordings stored on the Zoom cloud**
   - Settings → "*Recording*" tab → Enable "*Cloud Recording*"
   - Settings → "*Recording*" tab → Enable "*Only authenticated users can view cloud recordings*"
   - Settings → "*Recording Tab*" → "*Require passcode to access shared cloud recordings*"

5. **Delete all copies** of the recording stored either on the cloud or your device **when no longer required**.

6. Before sharing or posting the recordings, review them to make sure that the content is appropriate.