Hosting Secure Virtual Programs: Staff Guide

As March of Dimes Canada moves forward in increasing our virtual program offerings, ensuring client privacy and a safe and secure virtual meeting space are paramount concerns. This document provides guidance for MODC staff who are administering and hosting virtual group-based programming, so that you can manage privacy and security considerations while delivering a positive in-program experience for participants.

Please note: The guidance provided in this document applies to programs that do not require personal health information[1] (or other sensitive information) to be shared in the virtual environment. For programs where this type of information may be shared, consult Zinnia Batliwalla, Privacy Officer, for guidance at zbatliwalla@marchofdimes.ca.

Approved Technology

MODC has approved the use of Zoom for virtual programs.

All Zoom sessions must be hosted using an MODC Enterprise account. To request an Enterprise account, please contact Todd Thornhill at tthornhill@marchofdimes.ca. Once the account is created, you'll receive email instructions to activate it.

You can access Zoom through the web (us.zoom.com), a mobile app or desktop client. If you are using the app or client, please install all updates so you are always using the latest version.

The Zoom website offers a range of resources and tutorials to assist you in navigating the platform and hosting your meetings. Check out the Zoom Help Centre for video tutorials, how-to's and tips.

Configure Your Zoom Settings

When hosting a virtual program using Zoom, it is important to configure your settings in the following way. After making these changes once, they will apply to all your meetings.

If you are using the mobile app, you will need to access your account on the web or desktop client to make these changes.

1. Access your meeting settings

[1] **Personal health information** includes oral or written information about the individual, if the information: relates to the individual's physical or mental health, including family health history; relates to the provision of health care, including the identification of persons providing care; is a plan of service for individuals requiring long-term care; relates to payment or eligibility for health care; relates to the donation of body parts or bodily substances or is derived from the testing or examination of such parts or substances; is the individual's health number; or identifies an individual's substitute decision-maker. *(Ontario Information & Privacy Commissioner, 2020)*

- On the web (us.zoom.com):
    - Log into your account
    - Select “My Account”
    - Select “Settings”
- On the desktop client:
    - Log into your account
    - Select the “Settings” icon
    - Select “View more settings” to be taken to the main Settings page on the web

2. Adjust your settings as follows:
    - Join before host: *Disabled*
    - Participants video: *Disabled*
    - Require a meeting password: *Enabled*
    - Mute participants upon entry: *Enabled*
    - Waiting room: *Enabled*
    - Prevent participants from saving chat: *Enabled*
    - Private chat: *Disabled*
    - Co-host: *Enabled*
    - Screen sharing: *Only host can share*
    - Annotation: *Disabled*
    - Whiteboard: *Disabled (unless necessary for accessibility reasons)*
    - Remote control: *Disabled*
    - Allow removed participants to rejoin: *Disabled*
    - Far end camera control: *Disabled*
    - Allow participants to rename themselves: *Disabled*

Registering and Authenticating Participants

Zoom links or login information for MODC virtual programs should not be published on the web or in social media. Instead, participants should be directed to email a designated program lead/administrator to register for the program.

Program leads/administrators are responsible for authenticating registration requests before sharing login details. This may involve consulting databases or program lists to confirm the individual is a registered MODC participant, or reaching out to the participant directly to confirm their identity.

When you have authenticated the registration request, you can forward program details, including Zoom links and passwords, to the participant by email. Also attach the “MODC Virtual Programs: Participant Instructions” document to your email.

Hosting and Running Your Zoom Session

It's showtime! Here's how you can maximize privacy and security while your Zoom session is running:

- Use an MODC-issued device or computer to log into Zoom and host the session.
- Find a quiet location away from other people, so that you and the session participants are not overheard.
- Double-check that key Zoom security features are enabled:
    - Select "Mute participants on entry" (if not already selected)
    - Deselect "Allow participants to unmute themselves"
- 5 minutes prior to the program start time, allow participants to enter from the waiting room:
    - When authenticated participants enter the waiting room, allow them to join. At any time, you can unmute participants from the "Participants" menu.
    - If someone in the waiting room has an unknown/generic name (e.g. iPad), allow them to join and send a private chat asking for their full name. If they are on the registration list, welcome and unmute them; if not, ask them to leave and register for a future session.
- During the meeting, monitor all participants on screen by selecting the "Gallery View" option.
- If there are multiple MODC staff members attending the session, consider assigning a co-host so that you have additional support in managing the meeting. In the "Participants" menu, hover over the person's name and select "More," then select "Make Co-Host." If you are using the mobile app, simply tap their name and select "Make Co-Host."

Handling Incidents

MODC always strives to create an environment supporting personal goals, dignity and self-respect. We will not tolerate harassment, discrimination or bullying of any kind, in any forum – including virtual programs.

If an incident occurs during a virtual program, you must immediately take the following steps:

1. Stop and end the incident
    - Immediately remove the offending individual from the Zoom session. In the "Participants" menu, hover over the person's name and select "More," then select "Remove."
    - If you are using the mobile app, simply tap their name and select "Remove."

- If not possible to remove the individual, end the meeting, log in again immediately and lock the meeting.

2. Notify your supervising Manager/Director, and/or Vice President as appropriate

3. Provide an Incident Report to your direct supervisor