HOSTING ZOOM CONFERENCES

ZOOM SAFETY CHECKLIST:

BEFORE MEETING:
Disable autosaving chats
Disable file transfer
Disable screen sharing for non-hosts
Disable remote control
Disable annotations
Use per-meeting ID, not personal ID
Disable “Join Before Host” - Enable “Waiting Room”

DURING MEETING:
Assign at least two co-hosts
Mute all participants
Lock the meeting, if all attendees are present

IF YOU ARE “ZOOM BOMBED”:
Remove problematic users and disable their ability to re-join when asked Lock the meeting to prevent additional disruption
Instructions for how to perform all of these steps are listed below.

SAFETY MEASURES FOR ZOOM MEETING HOSTS
WHEN SCHEDULING OR SETTING UP A MEETING YOU WILL HOST:

SET SAFE MEETING DEFAULT SETTINGS
On the Zoom Settings page, turn off participant controls:
1. Sign into Zoom.us.
2. Click on the Settings link on the upper right (it looks like a gear symbol).
3. On the right side of the page, turn off: autosaving chats, file transfer, screen sharing, and remote control.

ASSIGN A CO-HOST
For larger meetings, identify a co-host or two ahead of time whose role is to be a virtual room monitor and manage order during the meeting by managing the participants. Co-hosts are assigned during a meeting and cannot start a meeting.
1. Sign into Zoom.us.
2. Click on the Settings link on the left of the screen.
3. Scroll down to the Co-host option on the Meeting tab and verify that the setting is enabled.
4. Turn on Co-Host. If a verification dialog displays, choose Turn On to verify the change.

ASSIGN A PER-MEETING ID
DON'T USE YOUR PERSONAL MEETING ID
Avoid using your Personal Meeting ID (PMI) to host public events.
Your PMI is basically one continuous meeting - your personal virtual space; and once it is published, others can join at any time.

PREVENT SCREEN SHARING BY NON-HOSTS To prevent participants from screen sharing during a call, use the host controls at the bottom of the window, click the arrow next to Share Screen and then choose Advanced Sharing Options. Under "Who can share?" choose "Only Host" and close the window. You can also lock the Screen Share by default for all of your meetings in your web settings.

ENABLE THE WAITING ROOM
Before you start your meeting, enable the Waiting Room for your meeting. You and your co-host will then play an active role in choosing who to allow into the room through the participants list. Meeting hosts can customise Waiting Room settings for additional control, and can even personalise the message that people see when they enter the Waiting Room so they know they're in the right spot. This is a great way to post rules and guidelines for your event, such as screensharing or muting policies

DISABLE JOIN BEFORE HOST
Before starting a meeting, disable Join Before Host to keep users out before the host arrives. This is the current default, but double check to make sure that it is set for the meeting. When "Join Before Host" is enabled, anyone can enter at any time and create havoc with other participants before the meeting officially starts.

TURN OFF FILE TRANSFER
In-meeting file transfer allows people to share files through the in-meeting chat. Toggle this off to keep the chat from getting bombarded with unsolicited pics, GIFs, memes, and other content.

TURN OFF ANNOTATION
You and your attendees can doodle and mark up content together using annotations during screen share. Disable the annotation feature in your Zoom settings to prevent people from writing all over the screens.

ONCE THE MEETING STARTS:

MANAGE DISRUPTIVE PARTICIPANTS
The Meeting Participants window offers control over most aspects of your meeting and those attending.

LOCK THE MEETING TO PREVENT RE-JOINING OF REMOVED PARTICIPANTS
During the meeting, a host or co-host can click on the More and Mute All Controls at the bottom of the Participants List. When viewing the Participants List, click Lock Meeting (under More) to prevent other participants from joining the meeting in progress.

MUTE ALL PARTICIPANTS

During the meeting, a host or co-host can click on the More and Mute All Controls at the bottom of the Participants list. On the Participants List, click Mute All to mute all meeting attendees.

GENERAL COMPUTER SECURITY:

Ensure your computers have strong passwords with required letters, numbers and characters. Those passwords should be changed regularly,

Please also be especially wary of fake emails claiming to come from Zoom, Facebook, or other social media platforms and websites. These emails may be sent with criminal purpose, such as extracting users' data from your systems. Clicking on one of these fake links may well activate such criminal or extremist activity. If in doubt, do not open the email and do not click on the link. At all times, try to ensure that you are using virus scanners that are as up to date as possible. Discourage unnecessary taking of photographs and online postings of Zoom meetings, especially with the backgrounds and workstations of staff. There have been examples of people posting photos of screens/documents with sensitive data on them which give malicious actors further vulnerabilities to exploit.

Nottingham & Derby Methodist District – May 2020