GUIDANCE FOR SECURE LIVESTREAMING

SUMMARY

This CST advisory note is intended to help keep online conference applications, such as Zoom, as secure as possible from unwanted participants. This includes antisemites who have already caused hostile Zoom and Facebook disruptions against British Jews in recent days. These antisemitic disruptions have now been made public by the media, raising the probability of 'copycat' behaviour by other antisemites and troublemakers.

CST strongly advises all Jewish communal groups that are now using online conference applications to ensure that the security precautions outlined in this note are followed. We stress that the use of such conference applications, especially at this time, should certainly continue so as to help bolster communal spirit and quality of life. To date, disruptions have been relatively rare, but the expectation is that they will increase, meaning precautionary security measures and good habits need to begin now, so as to avoid unnecessary disruption, upset and unwanted publicity.

COVID-19, LIVESTREAMING AND ANTISEMITIC DISRUPTIONS

The current COVID-19 situation has resulted in many synagogues and Jewish communal groups using livestreaming for services and events over applications such as Zoom.

Some extremists, including here in Britain, have abused the open nature of these broadcasts to join and disrupt the online meetings by what is now being called, "Zoom Bombing". This means disrupting and live "spamming" the chats and video broadcasts. The perpetrators may be "bots" (i.e. robots programmed to send such messages), local or overseas antisemites, or online "trolls" and other trouble-makers.

One example of this occurred on Friday 27 March when a Shabbat service at a London synagogue was disrupted by racist and antisemitic material being posted in the chat function throughout the service.

Another London synagogue had messages placed on its Facebook group whilst watching a live event.

Other disruptions have occurred in the USA and elsewhere, including a Torah class and a webinar on antisemitism.

With Jewish communities (and indeed the rest of society) increasingly reliant upon Zoom and similar technologies, there is every likelihood that internet trolls, criminals and political extremists will seek to exploit the current situation.

Specifically, regarding antisemitism, CST's research has uncovered numerous examples of far Right extremists seizing upon the Coronavirus pandemic as a vehicle to spread their hate, incitement and conspiracy theories.

All of the above compels CST to ask that you please follow the guidance below, to the best of your ability.

STAYING SAFE WHEN HOSTING ZOOM MEETINGS:

Carefully consider where you post your invitations to Zoom meetings from, as that is where your meeting ID and password can be found by hackers.

You may wish to directly email your community members rather than fully and openly publicising your meetings. This would reduce the risk of unwanted people joining but will make it harder for friendly non-members to benefit from your activity. You will have to decide where to find the correct balance for your own activity, between making your online event available to as many people as possible; and ensuring a safe environment for those people who do want to participate.

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 "Zoombombed":

- 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.

LOCKING 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.

MUTING 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.