SECURING VIRTUAL MEETINGS FOR SCOUTING

INTRODUCTION

The purpose of this document is to identify *what* Scouters can do to be prepared for a virtual meeting using videoconferencing tools and *why*. This is to reduce the risks from bad actors who are a threat to youth protection, security, privacy, and meeting success. The phrase "bad actors" in this context is not judging theatrical skills in a campfire skit. Bad actors may include uninvited guests who intend to disrupt virtual meetings (also known as "Zoombombing") or invited participants whose behavior is not following the Scout Oath and Scout Law.

A certain amount of organized chaos during a virtual meeting is to be expected as Scouts and Scouters develop in character and leadership. Even the most basic measures to secure a virtual meeting may seem unnecessary to some—until an incident occurs. Be Prepared.

The terms and examples used in this document are based on Zoom because that is currently the most commonly used tool for virtual meetings; however, the concepts apply to all video conferencing tools. A Scouter who is hosting a virtual meeting is responsible for understanding the safe and appropriate use of the tools that they are using—whether conducting a unit meeting, a roundtable, or another BSA gathering.

SECURING A MEETING

Managing a videoconference for Scouting involves trade-offs between convenience, collaboration capabilities, and risks of misuse.

Securing a virtual meeting can be thought of in three stages:

1. Protect
2. Detect
3. Respond and Recover

PROTECT

The first stage of securing the meeting is to manage the known risks by taking proactive steps to protect participants (especially youth) and any information that they will be sharing.

Check for Software Updates

Ensure that the latest version of the app is installed before scheduling or hosting a meeting. This ensures that all known security patches have been applied. Encourage participants to check for available software updates before they join the meeting.

Scheduling a Meeting

- **Use a Generated meeting ID**—Don't use your Personal Meeting ID (PMI), which is a static number. Once your PMI is known by a bad actor, they can attack any meeting you are using with that ID.

- **Passwords**—Always use a password for the meeting. This adds a second piece of information that is required for access beyond just a meeting ID that can be discovered by automatically trying every possible number. Use a stronger password than the six numbers or characters that are the current default in Zoom.

- **Limit access to meeting credentials** required to join the meeting. The risk of misuse and uninvited guests increases the longer and more broadly the meeting ID and password are available. Methods to limit access include the following:
    - **Send just in time**—Send the meeting ID and password closer to the start of the meeting.
    - **Separate credentials**—Send meeting ID and password at different times and/or different channels (e.g., email and text). You are not restricted to using the default invitation text containing both the meeting ID and password that is generated by Zoom.
    - **Recurring meetings**—Don't schedule recurring meetings to use the same meeting ID and password. The convenience of reusing the same meeting ID and password can be outweighed by the increased risk of those credentials being distributed and misused the longer that they are valid. Schedule each meeting instance individually with a different generated meeting ID and password.
    - **Registration—**If you need to communicate a meeting to a broad set of potential invitees on a public site such as Facebook or a local council calendar, require those who wish to participate to preregister. Once approved, the participant will receive an email with a personalized link for them to join the meeting. Learn more about Setting up Registration for a Meeting.

- **Authenticated users**—It is possible to require users to have a Zoom account and to log in to that account before joining the meeting. This is not recommended in most cases. Many people who join Scouting meetings as participants do not have Zoom accounts. Requiring accounts and authentication has been observed to frustrate such users and result in lower attendance. Authenticating a participant by having them sign in to an account does not ensure that they are who they say they are. For example, it has been reported that credentials for over 500,000 Zoom accounts are available for purchase on the dark web.

- **Waiting room screen—**Edit the waiting room screen to identify rules for the meeting (such as the Scout Oath and Law; no recording) and any ramifications for unauthorized users joining the meeting such as removal and reporting to Zoom.

- **Start time and duration**—Providing 10–15 minutes of gathering time for conversation before the meeting formally starts and additional free time after it ends may reduce the risk of participants being disruptive during the meeting.

Settings

There are trade-offs between the following collaboration capabilities of the videoconferencing app and security or youth protection. Disable any capabilities not required for the meeting. If they are needed and enabled, teach participants their appropriate use in Scouting using the EDGE method.

- **Rename**—Allowing participants to change the name that is displayed for them in the meeting enables
    - youth to change it to First name Last initial (e.g., John D.), which prevents a screenshot of a meeting from including both a youth's picture and full name; or
    - adults to change their name to what the Scouts normally call them; but also
    - misuse by a participant to impersonate someone else (especially if their video is off); or
    - misuse by a participant to display something disruptive or inappropriate.

- **Waiting room**—Utilize the waiting room to screen participants attempting to join the meeting. Note that they may not be who they say they are. Two adult leaders must be in the videoconference to have two-deep leadership before admitting youth participants.

- **Participant audio**—This is a fundamental capability of videoconferencing, but it can be a source of inappropriate speech and disruption when participants are not on mute. Options include disabling participants' ability to unmute themselves.

- **Participant video**—This is a fundamental capability of videoconferencing, but it can be a source of inappropriate content in terms of behavior, clothing, and background.

- **Virtual background**—Enabling the participant to display a virtual background is a popular option and can add interest. Virtual backgrounds need to be monitored by the host and co-hosts for Scouting-appropriate content.

- **Recording**—The ability for the host, co-hosts, or participants to record the meeting should be disabled in the videoconferencing tool to comply with BSA policy. Be aware that resourceful participants could still use screen capture or third-party recording apps. Depending on your meeting participants, it may be advisable to include a statement on the waiting room screen that recording and screenshots are not allowed and/or verbally emphasize it during the meeting. Consent must be obtained in cases where recording is allowed by BSA such as a virtual camp run by a local Council. Learn more about How to Prevent Recording in Zoom.

- **Screen share**—Options include disabling screen sharing by participants (i.e., limiting screen sharing to host or co-hosts) and only allowing the host or co-host to start sharing when someone else is already sharing. Limiting screen share capabilities to the host and co-hosts prevents participants from sharing inappropriate material or sharing at a disruptive time. If a participant legitimately needs to share their screen, they can be made a co-host temporarily.

- **Chat**—Chat can be useful to ask questions or to share additional information related to the current meeting topic; however, it can also be misused to share unrelated or inappropriate content, or for discourteous side conversations.
  - Options include disabling chat entirely, or allowing participants to chat with:
    - no one;
    - host (or co-host) only one-to-one (1:1);
    - everyone publicly; and
    - everyone publicly or privately (1:1).
  - Youth should not be sending chat messages 1:1 with an adult. If chat is enabled, at least two adults must be included on messages with youth, which may require messages to be sent to everyone publicly. If a 1:1 question is received by an adult from a youth, redirect the youth, and if appropriate, communicate the question and answer to everyone.
  - Be careful of what is sent to everyone. Keep the content in chat to the meeting topic.
  - A Scout is Courteous, so chat should not be used for side conversations.
  - Chat should not be used to communicate personal or other sensitive information.
  - There are also options to enable or disable saving of the chat text to a log. A chat log can be helpful to follow up on questions that were not answered during the meeting or to review conversations that occurred between participants.

- **File transfer**—It is recommended to disable this feature in chat, especially in meetings with youth. It can be misused to share content that is not appropriate in Scouting.

- **Breakout rooms—**Two-deep leadership is required in each separate meeting, including each breakout room.

- **Annotation**—Annotation can be used for productive collaboration by marking up shared screens, but it can also be misused for disruption. It is best limited to small groups.

- **Whiteboard**—Whiteboard can be used for productive collaboration or misused for disruption. It is best limited to small groups.

Joining a Meeting

- **Admit participants from the waiting room**—If the host (or co-host) sees someone in the waiting room who they do not know or if they are not sure of the participant's identity (e.g., same name as someone who already joined), they should confirm the person's identity by methods such as
  - sending a chat message to waiting room;
  - communicating via another channel such as text, phone, or email; or
  - admitting the participant to the meeting and immediately checking video for identity.

During a Meeting

- **Lock meeting**—Once the meeting has started, the host can prevent anyone else from trying to join; however, this can be a problem if a participant is late or drops from the meeting and needs to join in again.

DETECT

During a meeting, hosts and co-hosts need to monitor to detect incidents such as uninvited guests or content that is inappropriate in Scouting. Despite the host's best efforts at preventing incidents, they can and will occur. It is very difficult for the same person to lead a meeting and perform all of the hosting responsibilities, so it is recommended to

- assign co-host(s); and
- have a duty roster to assign areas for the host and each co-host to monitor.

Areas to monitor for incidents include the following:

- Participants in the waiting room seeking to join the meeting
- Video of each participant, including their behavior, clothing, and background
- Audio of each participant
- Participants' displayed names
- Chat
- Screen share
- Breakout rooms
- Annotation
- Whiteboard

RESPOND AND RECOVER

If an incident is detected, the following responses can be taken in increasing order of severity. These responses can approximate what would occur during an in-person Scouting meeting.

- Remind all participants of appropriate behavior according to the Scout Oath and Law.
- Turn off one or more participants' video and/or mute their audio.
- Speak to one or more participants off to the side in an online breakout room (maintain youth protection barriers to abuse with two-deep leadership and no one-on-one contact).

- Place participant back in the waiting room (for a time out, or to confirm their identity via a separate communications channel such as text, phone, or email).
- Remove participant from the videoconference with no option to return.
- End the meeting for all.

Always follow Youth Protection reporting procedures including mandatory reporting of child abuse and reporting of violations of BSA Youth Protection policies.

After the Meeting

- Request Start-Stop-Continue feedback.
- Review any incidents, how they were detected, and the responses to them.
- Review participant attendance report and chat log (if saved).
- Make any needed procedural and settings changes to improve before the next meeting.
- Communicate changes.

REFERENCES

- BSA Digital Safety and Online Scouting Activities—https://www.scouting.org/health-and-safety/safety-moments/digital-safety-and-online-scouting-activities/
- BSA COVID-19 FAQ—https://www.scouting.org/coronavirus/covid-19-faq/
- BSA Youth Protection—https://www.scouting.org/training/youth-protection/
- How to Prevent Recording in Zoom—https://www.scouting.org/wp-content/uploads/2020/11/How-to-Prevent-Recording-in-Zoom.pdf
- Privacy and Security for Zoom Video Communications—https://zoom.us/docs/ent/privacy-and-security.html
- Setting up Registration for a Meeting—https://www.scouting.org/wp-content/uploads/2020/11/Setting-up-Registration-for-a-Meeting.pdf
- Successful Virtual Meetings—https://www.scouting.org/wp-content/uploads/2020/11/Successful-Virtual-Meetings.pdf
- Zoom Security—https://zoom.us/security