PRIVACY AND VIDEO/ONLINE CONFERENCING GUIDELINES

Best Practices for Hosts

Regardless of the video conferencing service you choose to use, if you are hosting the meeting, you must ensure you have all the appropriate privacy and security settings in place.

Follow these privacy and security best practices when scheduling a meeting, and during and after the meeting, to maintain a balance between privacy and business requirements.

Scheduling

- Ensure meeting links are distributed only to the relevant attendees.
- Keep titles generic and do not include any personal or confidential information.
- If the meeting has external participants use a password to secure the session if possible.
- Request that meeting invites not be forwarded without permission.
- Ensure anyone entering the meeting as a “guest” verbally identifies themselves before you begin.

Waiting Room/Lobby Features

Most video conferencing tools have a waiting room feature that will require the host to approve participants before they can join. This feature should always be enabled, especially if you are using the tool with external organizations or third parties, as it allows you to screen participants to ensure everyone that wants to join the meeting was invited. This prevents unwanted individuals from joining your call and immediately having access to audio and video. You should also enable any setting that ensures participants cannot join before the host if the meeting software you are using supports this option.

Meeting Lock Features

Some software features a “lock” feature that will allow the host to prevent anyone from joining the meeting after the lock has been applied. As soon as all participants have joined the meeting the lock feature should be used to secure the meeting room and prevent any unauthorized entry.

Recording

While most video conferencing software offers the ability to record sessions, this feature should **not** be used unless required for business purposes. If recording is required, only the meeting host should be recording the session. It must never be used for one-to-one meetings which discuss personal information or HR related issues. If recording is to be used, opt for a **local recording storage** option which will keep the files on your work computer. Recordings are records and need to be managed accordingly and will need to be produced if there is a FOIPOP request. Consider uploading presentation slides rather than recording sessions.

Chatting

Many video conferencing tools offer the ability to chat during meetings. Chat retention varies from program to program and based on the meeting type. For example, the chat of a personal meeting room may persist over a long period of time, whereas the chat for a single session meeting may be deleted once the meeting ends. The chat feature should not be used for formal discussions. Also keep in mind that the chat should not constitute documentation of a decision; not all chats are saved. Chats should not be relied upon to document meeting content. Participants should be dissuaded from using chat in lieu of actively participating in the meeting to verbally share comments.

During the Call

- At the outset of the meeting a quick roll call is a good way to validate user identity.
- Do not share any personal or sensitive information until you are sure only the participants that have been invited to the meeting are in attendance.
- Screen sharing during the meeting is okay but be mindful of what other documents you may have open before doing so. Limit who can share their screen if possible.
- If you are sharing a file, notify participants you will be doing so and what the content of the file is.
- Always be aware of what is in the background of your webcam if you are using video, especially if working remotely. Use a space that is private.
- Mute your microphone when not speaking and remind others to do the same.
- If recording has been enabled, ensure others not part of the meeting are not captured on the video or audio recording.
- If you initiate recording, you must notify all participants that the session is being recorded. Recordings should always be stored on a local drive. Ensure that you know who has access to the recordings. Delete recordings in accordance with your records retention schedule and always after they have served their purpose.

After the Call

- Ensure you have disconnected from the call and are no longer broadcasting video or audio
- Make sure any important decisions made during the meeting are properly documented.
- If recording was used, then you must maintain these as a record and manage them accordingly.

For more information:
privacy@smu.ca

Adapted with permission from: Information Access and Privacy (IAP) Services
Department of Service Nova Scotia and Internal Services, April 2020.