KEY ZOOM HEALTH AND SAFETY MEASURES

Zoom is designed to facilitate virtual meetings at work and at school, and many of its features are not in keeping with Al-Anon principles. Most of these features pose security risks for devices lacking the added protection of a cybersecurity system supported by an IT team. Some features can be distracting, compromise anonymity, or trigger health problems for certain participants.

To determine whether to activate a feature, always ask the question: "Is there anything equivalent to this, either encouraged or discouraged, in an in-person Al-Anon meeting?"

The Al-Anon/Alateen Service Manual and our Legacies remind us of the role of meetings in carrying the message, of the necessity for good leadership at all service levels, that the fellowship of our groups shall remain democratic in thought and action, and that personal progress for the greatest number in recovery depends upon unity.

HIGHLY RECOMMENDED FEATURES

Waiting Room	Invaluable hosting team tool; if overridden by group conscience for those arriving for the meeting, the host can activate it during the meeting to manage challenging participants. NOTE: For security purposes, Zoom imposes a waiting room on any meeting without a passcode and removes the ability for anyone to join that meeting before the host.
Passcode	Essential security measure; if a newcomers/beginners' meeting is created without a passcode, Zoom will impose a waiting room on that meeting. NOTE: For security purposes, Zoom discourages the posting of passcodes on websites or social media platforms.
Stop/Start Video	Participants should have the ability to stop video when they are doing something distracting and to restart video when they are settled. If a member of the hosting team stops the video, it requires cooperation between a hosting team member and the participant to restart video again.
Chat (limited by Host)	Chat should never be set to "No One," as this cuts off all communication between meeting participants and the hosting team. For most of the meeting, set Chat to "Host and co-hosts," which allows direct communication between a member of the hosting team and one participant at a time or everyone in the meeting. During the last 15 or 20 minutes, change Chat to "Everyone" for open communications between any one member and the group. Private Chat ("Everyone and anyone directly") is strongly discouraged, as it is a favored tool of hackers, infiltrators, and disruptors. Also, there is no reason or opportunity for a Private Chat during an in-person Al-Anon meeting.
Polls	Excellent tool for gauging interest in a business meeting topic or taking a final (anonymous) group conscience vote; requires notable involvement by the group's Zoom Account Administrator.
Closed Captions / Transcription	We wish to ensure access to our meetings (virtual or in person) by everyone, and "Live Transcription" is a fairly new Zoom feature that can be activated as an available option (with subtitles turned off or on by each participant) for those who are hard of hearing.

FEATURES TO CONSIDER VIA INFORMED GROUP CONSCIENCE

Non-Verbal Feedback	When this feature is toggled OFF in administrative settings, the Raise Hand/Lower Hand icon is still visible on the Zoom menu bar. The question to ask is: "Does our group need the "Yes" and "No" voting icons during our meeting?" (This is true at a district level but may not be needed at the group level.)
Muting/Unmuting	For a smaller meeting with a responsive hosting team, participants can mute and unmute themselves. For a larger meeting, the group may decide that meeting participants should raise their hands and then be unmuted by the hosting team as they are called on in turn to speak.
Lock Meeting	Locking the meeting before Chat is opened to Everyone is recommended as a security precaution. If participants are getting bounced out of the meeting due to technical difficulties related to weather or other conditions, the Host has the prerogative (by group conscience) to unlock the meeting so someone can return or to leave it unlocked. The hosting team remains particularly vigilant under these conditions.

STRONGLY DISCOURAGED FEATURES

	REASONS			
ZOOM FEATURE	Security Risk	Health Threat	Not in Keeping with Program Principles	**DETAILS**
Virtual/Blurred Backgrounds	✓	✓	✓	Favored disruption tool; open door to hackers; can cause seizures, migraines, vertigo, or nausea; challenging for hosting team; contributes to Zoom fatigue; essentially a toy (nothing equivalent at in-person meetings)
Video Filters			✓	Challenging for hosting team; contributes to Zoom fatigue; essentially a toy (nothing equivalent at in-person meetings)
Sending Files via Chat	✓			Open door to hackers; if overridden by group conscience, lock meeting before posting file
Screen Sharing	✓	✓	✓	Favored disruption tool; open door to hackers; screen sharing meeting readings is a copyright violation; can cause seizures, migraines, vertigo, or nausea; contributes to Zoom fatigue; nothing equivalent at in-person meetings
Screenshots			✓	Violation of anonymity
Save Chat/Captions			✓	Violation of anonymity

STRONGLY DISCOURAGED FEATURES

ZOOM FEATURE	REASONS			DETAILS
	Security Risk	Health Threat	Not in Keeping with Program Principles	
Renaming Self in Meetings	✓			Favored disruption tool; participants can confirm their names in the box under the Meeting ID while joining a meeting and the hosting team can make changes during the meeting
Recording/Saving Recordings			✓	Violation of anonymity
Profile Pictures			✓	Challenging for hosting team; contributes to Zoom fatigue; violation of anonymity
Private Chat	✓		✓	Favored disruption tool; creates harassment, gossip, or crosstalk opportunity during meetings; no reason or opportunity for Private Chat at an in-person meeting; may be opened during after-meeting fellowship if the group insists
Personal Zoom Accounts	✓		✓	Only the group's Zoom account should be open during the meeting; additional Zoom accounts create an inviting doorway for hackers, infiltrators, and disruptors; violation of anonymity
Open Browser/Other Software	✓			Open door to hackers; bring published meeting readings or open these documents with a separate device
Meeting Reactions			✓	Distracting and equivalent to crosstalk
Meeting Links	✓			Do not invite anyone to a meeting with a link; instead, send the Meeting ID and Passcode to join the meeting through the Zoom app
Join Meeting via Browser	✓			Open door to hackers; using a browser to start or join a meeting excludes access to some features, including security; the best and safest way to start or join a meeting is through the Zoom app
Join Before Host	✓			Open door to hackers, infiltrators, and disruptors

STRONGLY DISCOURAGED FEATURES

ZOOM FEATURE	REASONS			DETAILS
	Security Risk	Health Threat	Not in Keeping with Program Principles	
Integration of Outside Apps	✓			Open door to hackers, infiltrators, and disruptors
Immersive View	✓	✓	✓	Potential disruption tool; open door to hackers; can cause seizures, migraines, vertigo, or nausea; contributes to Zoom fatigue; essentially a toy (nothing equivalent at in-person meetings)
Host Key	✓			Profound security risk in regular meetings (designed for Zoom Rooms) with potentially cascading consequences
Focus Mode			✓	Draws unnecessary attention to the hosting team
End-to-End Encryption	✓			Not necessary (unless dial-in access is allowed); enhanced encryption (standard on Zoom) is sufficient for an Al-Anon meeting
Dial-In Access	✓			Breaks encryption for all other participants in the meeting
Breakout Rooms	✓			Favored tool for hackers
Avatars		✓	✓	Challenging for hosting team; contributes to Zoom fatigue; may cause seizures, migraines, vertigo, or nausea; essentially a toy (nothing equivalent at in-person meetings)