10 tips for safe online meetings and collaboration

1. Manage your meetings
   - Control and set meeting participant settings for a specific meeting you’ve created.
   - Determine who can bypass the lobby, who can present content, and if attendees are muted by default.

2. Decide who can join your meeting
   - Set which participants can join your meeting directly and who needs to be admitted via the lobby.
   - Specify in meeting options who can bypass the lobby in meeting options.

3. Control who can present their screen or content
   - Decide which attendees will have a presenter role and who will join as standard attendees.
   - Specify in meeting options or during a meeting open the participant pane and select a participant.

4. Mute all meeting attendees
   - Place a hard mute on all attendees to keep the meeting focused on the presenter preventing disruptions.
   - Specify in meeting options all participants are muted, or with the presenter role open the participant pane and select don’t allow attendees to unmute.

5. Mute or unmute individual attendees
   - Manage attendees who may need to be muted or unmute an attendee during a hard mute meeting.
   - In the participant pane select a participant to mute or allow to unmute.

6. End the meeting for all attendees
   - As the meeting organizer, end the meeting or all attendees instead of leaving the meeting open.
   - Once a meeting has wrapped up, instead of Leave select the arrow dropdown and click End Meeting.

7. Use 1:1 chats when applicable
   - Use 1:1 chats to discuss information that shouldn’t be shared across an entire team.
   - Create a new chat and add the appropriate member.

8. Create a private channel to limit members
   - Setup a private channel within an existing team to keep sensitive information limited to those private team members.
   - Add a new channel within a team and specify the privacy to be Private.

9. Create sensitivity labels to keep teams secure and private
   - Create a new team and apply a sensitivity label to restrict membership and protect content.
   - Create a new team and in the sensitivity drop down, select the appropriate classification label.

10. Recognize when business-sensitive information may have been inadvertently shared
    - Teams supports data loss policies to help protect sensitive information from being accidentally shared.
    - In a 1:1 chat or channel conversation, if a message is blocked select What can I do? to view the policy tip to understand why that content shouldn’t be shared.