Darla Moore School of Business

Information for Potential Zoom Users: Differences between Zoom and Collaborate & Implementing DMSB Policies when Using Zoom

Robert Lipe

August 2020

Information for Potential Zoom Users:
Differences between Zoom and Collaborate &
Implementing DMSB Policies when Using Zoom

Revised 8/8/2020

For Fall 2020, DMSB has decided that nearly all classes will be livestreamed. Also, if a class is livestreamed, it should be recorded and the recording made available to students. Extensive training materials have been created for livestreaming with Blackboard Collaborate Ultra. A variety of training sessions on the use of Collaborate have/will be offered to faculty.

However, DMSB policy allows faculty to livestream with Zoom instead of Collaborate. The purpose of this document is to help faculty make an informed choice between the two platforms. It is divided into two sections:

Section 1 identifies some key differences I have observed regarding what faculty and students would experience between using the two platforms, and

Section 2 provides some suggestions on Zoom settings a faculty member should select to be consistent with DMSB livestreaming policies if using Zoom in Fall 2020.

Note that information in this document focuses on small classes because DMSB anticipates that Zoom will only be used for heavily discussion oriented classes where gallery view is beneficial. For really large livestream sessions, both platforms require instructors to use "Webinar Mode". Information about Collaborate's Webinar Mode (required for sessions with more than 250 attendees) can be found in your department sandbox livestream training materials.

Part 1: Key Differences between Using Zoom and Collaborate at DMSB:

If Zoom and Collaborate were both equally integrated into UofSC's learning management system (Blackboard), if the two were equally supported by University and DMSB IT services, and if both were free to all faculty and students, I estimate that 70-80% of instructors would use Zoom. However, Collaborate is integrated into Blackboard and free for us to use; Zoom is neither of those things. Also, faculty using Collaborate will have extensive IT support, whereas faculty using Zoom will need to expend extra effort to do a lot of IT support activities on their own. For that reason, I expect most faculty will prefer to use Collaborate.

Other than integration and support, the two platforms are more similar than different in my opinion. If the instructor selects the proper settings in either platform, everyone can see the person who is talking, the instructor or a student or a guest speaker can share content with the rest of the class, the students can be split into breakout groups, students can raise their hands, etc. On the whole, several features of Zoom are more user friendly than Collaborate. Zoom also has a ton of options (as shown below) which makes it flexible but also potentially difficult to operate for those unskilled in livestreaming a class. In part because of the lack of integration with Blackboard, Zoom poses more security risks.

1. Security: No system is ever fool-proof, but security in Collaborate seems easier to implement.

   Collaborate: The recommended DMSB approach is to have students enter the virtual classrooms using their Blackboard credentials and **not** to distribute the Collaborate room guest link to students. Thus user access is controlled by UofSC authentication service, and no faculty effort is required to secure their room.

   Zoom: Faculty have to take additional steps to make sure only students or guests who they want to admit will be allowed to enter the room. Some recommended solutions can be a burden on faculty and must be done before every class session. For example, if the faculty uses the waiting room feature in Zoom from a first-floor classroom with a large number of streaming students, then in addition to turning on the AV, loading their materials, and starting Zoom, they will also have to be analyzing if people in their waiting room are a valid students or a Zoom-bomber. The second part of this document discusses expectations about room security for instructors choosing to use Zoom.

2. Seeing webcam video of students: This is perhaps the most well-known difference due to the gallery view feature in Zoom.

   Collaborate: When not sharing content, the instructor is only able to see 4 webcams from students. The 4 represent the students who either entered the session first or who most recently made a noise while their mics were unmuted. When content is being shared, the default is for the content to be big and the active speaker to be a small thumbnail at the lower right. A participant can click the thumbnail and make the speaker big and the content small.

   Zoom: When not sharing content, the instructor can see a large gallery view with the potential to scroll through the webcams of every participant, assuming they turn on their webcams. This is a very popular feature when holding meetings or social gatherings. The usefulness of this in a classroom setting will depend a lot on the specific course. When content is being shared, the user can see content and active speaker; depending on what settings the user selects as well as how the user joined the Zoom meeting, the user can see some of the non-speaking attendees as well. For small classes which are focused heavily on discussion, the ability to see more than 4 students is very useful. For a large class or a class where the instructor generally is sharing content, this feature seems less valuable.

3. Recording the class: Per DMSB policy for Fall 2020, faculty will need to record livestreamed classes, and the recordings should be kept in a secure location that allows streaming but not downloading. Complying with this guidance requires more effort when classes are livestreamed in Zoom. Section 2 provides more details of how recordings in Zoom should be made available to students.

   Collaborate: Recording requires clicking a button to start and clicking a button to end. The recording is stored in Collaborate. In order to secure these class session recordings, DMSB recommends that the recordings remain in Collaborate and students not be allowed to download the videos, which is a setting in Collaborate. Other than making sure the students know where to find the replays, the faculty member does not need to do anything with the recordings. No files need to be downloaded or uploaded. At most, the faculty member might rename the recording to make it easier for students to access the session recording they want.

   Zoom: Faculty will need to record to their local computer if livestreaming from home or to the Zoom cloud if livestreaming from the first floor. If using the Zoom cloud, the video files will be very large

and faculty member Zoom accounts will run out of space after about 2 class sessions. Thus, cloud recordings will have to be downloaded to the faculty's computer or One Drive. From there, recordings made from home or from the first floor have to be uploaded to a storage space where they can be securely viewed by students. Uploading time depends on the size of the file and the faculty member's internet upload speed; some cloud recordings take 3 hours to upload from my house but a fraction of that time from my office computer. In addition, the faculty member needs to link the recording to Blackboard where students can find it without being able to download it.

4. Controlling functions during class: Effective livestreaming is often enhanced by being able to control room functions from a "persona" other than the one doing the livestreaming. For example, the faculty member could enter the virtual room twice, which I call having a "second persona." Or a TA can enter the room and be given authority to control the virtual room.

   Collaborate: It is easy for the instructor to set up a second persona on a laptop and give that persona full moderator rights. Alternatively, it is very easy to give a TA in the virtual classroom moderator rights. This is very helpful when running class from a computer with a single monitor, such as the first floor of DMSB. Specifically, the faculty member can have a laptop with which he/she monitors chat, the raised hands, and launches polls or breakout groups while sharing full screen content from the desktop monitor to both the remote students and the F2F students.

   Zoom: Creating a second persona is less straightfoward. Also, Zoom allows additional co-hosts but only one host, and certain functionalities, such as putting people in breakout groups and starting the groups, can only be performed by the host. Using a TA or a laptop to set up breakout groups and other tasks reserved for the host requires swapping the role of host between instructor, the instructor's second persona, and/or the TA.

5. Guest speakers: Both systems allow you to share a link with a guest speaker and have them join the session. If appropriately configured, both systems allow the guest speaker or a selected student to present materials from their computer to the rest of the participants in the session. However, there are some subtle differences.

   Collaborate: Attendees have one of 3 roles - participant, presenter, or moderator. A moderator can change an attendee's role during the session. A moderator can change any setting within the virtual room; students should not be given moderator rights. Presenters can turn on audio, video, and share their screen. This is the proper role for a guest speaker or for a student who is to present materials from his/her computer to the class. Participants cannot share the contents of their computer screen; whether they can share their audio, webcam video or type chat messages is determined by the settings selected by the instructor.

   Zoom: Attendees have one of 3 roles - participant, co-host, or host. A student presenter or guest speaker could be assigned the role of co-host. In addition to being able to turn on their microphone, video, and share content, the co-host has a lot of power in a Zoom meeting, such as being able to kick students out of class. This is a lot of power to turn over to a student. If you assign a student presenter to be co-host, I recommend you return them to being a participant immediately after their presentation concludes. The alternative in Zoom is to assign student presenters or guest speakers to be regular participants but give EVERY participant in the session the right to share their audio, video, and content. For small classes with reasonably mature students, this may be a reasonable solution, but it comes with some risks of someone sharing something inappropriate,

such as their attempt at a graded homework problem. The presenter role in Collaborate seems to fit guest speakers and student presenters better than any alternative I can find in Zoom.

As an aside, Zoom allows only one host whereas Collaborate allows multiple moderators. The limit of a single host can create problems in Zoom if you want a TA or your second "persona" on your laptop to initiate certain actions in Zoom that are reserved for the host only (e.g., creating polls or assigning breakout groups).

6. Preparing prior to class: Both systems allow instructors to launch polls and use breakout groups. But they differ regarding whether these can be set up in advance.

   Collaborate: A class session is very "transitory". For example, you can create polls in a class session (and the results are saved in Blackboard), but you cannot create the poll questions and answers in advance of the session. You can type the questions in Word in advance and copy/paste them into Collaborate during class. For breakout groups, you can assign students to a breakout group during the session but not before the session, and if you stop and restart breakout sessions during class, the group membership in the second breakout will not be the same as in the first breakout; we have devised some work-arounds for this, one of which is to allow students to pick their groups.

   Zoom: A class session has more "memory" in that you can set up breakout groups in advance if you know information about how the student will log in (they do not log in to Zoom with UofSC credentials). However, it is impossible to let students choose their group unless you make everyone a co-host. You can also set up polling questions and answers in advance.

Part 2: Choosing Zoom Settings that Comply with DMSB Livestreaming Policies

This part of the document discusses various settings for Zoom, along with observations about which settings are needed to comply with DMSB policies for Fall 2020. Some of the default settings are likely to be incompatible with our livestreaming policies, so Zoom cannot simply be used as is. Zoom has a lot of flexibility, but that means the program has a significant number of optional settings, which also means this section is really long.

To access these settings, I went to my Zoom profile, clicked SETTINGS, and then clicked on MEETING settings and RECORDING settings. Because (i) Zoom has optional settings that cover a lot of features, (ii) DMSB does not provide any training on Zoom, and (iii) whether/how some of the options relate to livestreaming your class is not obvious, this section reviews each and every setting for Meeting and Recording that appear in my Zoom profile on 8/4/2020. Do direct your attention to key settings:

- Any setting that I view as being mission critical appears in a box with double-line borders
- Any setting that is important but not mission critical appears in a box with regular borders.

I do not include options related to Telephone, because that seems unlikely to apply to livestreaming a class using Zoom.

A. ***Meeting settings related to security***: Based on UofSC guidance, posting a single link to a Zoom classroom that anyone can use for the entire semester does not provide the type of classroom security that DMSB expects. The following measures come from DoIT:

Do not make meetings or classrooms public. In Zoom, there are two options to make a meeting private: require a meeting password or use the waiting room feature and control the admittance of guests.

Do not share a link to a teleconference or classroom on an unrestricted publicly available social media post. Provide the link directly to specific people.

Manage screensharing options. In Zoom, change screensharing to "Host Only." If screensharing is needed by another individual (ex. Presentations), only provide that permission to the individual for that specific time period.

Ensure users are using the updated version of remote access/meeting applications. A recent update to the Zoom software, for example, both removed vulnerabilities in the application and enhanced the software with additional security features.

Review of security settings:

1. **Waiting room:** many sources recommend this for security. However, for a large class of students who might log into Zoom using a variety of names, trying to decide who to admit and who to deny in those precious minutes at the start of class might be vexing. This is especially true if you are using the brief times between classes to set up in a first floor classroom. You can admit multiple students at a time using Admit All, which lets everyone currently in the waiting room into the class session. If you have a TA, you have them manage the waiting room, but again, you will need to give your TA an accurate list of Zoom login names.

2. Require passcode when scheduling new meetings: Passcodes for meetings add security as long as you and the students keep them secure. Changing the passcode for every class is probably most secure, but that means you have to deliver the codes to students in a sufficiently timely manner for them to use the code to enter that specific class session.

3. Require passcode for instant meetings: because a livestreamed class will be a scheduled meeting and not an instant meeting, this seems irrelevant to livestreaming

4. Require passcode for Personal Meeting ID: my understanding is that you should not hold class in your personal meeting room (the room accessed by your PMI). If so, this setting is irrelevant to livestreaming.

5. Embed passcode in invite: simplifies the task of a student joining using an invite link. But if the invite link is made public by a recipient, the passcode does not offer much protection.

6. Require passcode by phone: I am unsure who would be joining a livestream class by phone. For security, it makes sense to require a passcode.

7. **Only authenticated users can join meetings**: I like this option for several reasons. First, no one can enter the classroom without successfully logging into Zoom. If someone who logged in causes trouble, it will be easier to identify the culprit. Without this, if I have your classroom link, I can get into your class (or waiting room if you use one) without verifying my identity. If I know who is in your class, I can enter the room with their name and likely be admitted from the waiting room into your class session.
   Second, if you plan to preassign breakout groups or ask polling questions for a grade, you have

to have some way to identify students. Because Zoom is not integrated with BB, you cannot use BB IDs for this. But if you require your students to give you their email address or user name that is associated with the Zoom account they use when attending your course, you can match those Zoom user names to BB IDs.

8. Only authenticated users can join meetings from web client: This setting appears to apply to the subset of users who join using the web without downloading the zoom software. If (7) is on, I think this setting is irrelevant. If (7) is off, then turning (8) on would stop my ability to get into your room while spoofing a student as mentioned in (7).

Review of settings related to scheduling a meeting:

9. Host video: do you want your camera on automatically or not?

10. Participant video: turn this off. You do not want to see them until they are ready to share. Indeed, you might want to disable their video until you are sure no intruders are in the room. They could send an unpleasant image to your students via their webcam.

11. Audio type: many students have more sophisticated audio devices for their phones than for their computers. My experience with Collaborate is that 5-10% will choose to join with their telephone, so I would allow this. Warning: I do not know what happens when someone who calls in on their phone is put into a Zoom breakout group; does their phone audio go with them, or is phone call considered a different user than their computer session, in which case their phone gets put in one group and their computer in a different group?

12. **Enable Personal Meeting ID**: should **not** be used for livestreaming.

13. **Use PMI when scheduling a meeting:** PMI should **not** be used for livestreaming.

14. Use PMI for instant meeting: PMI should not be used for livestreaming.

15. **Mute participants on entry**: Turn this **on**. Without doing so, as soon as a person joins, their mic is "hot" which leads to a lot of distracting noise. You can control when participants can unmute from inside of the meeting.

16. Upcoming meeting reminder: not sure what this does

B. ***In Meeting settings***: these settings can be set in advance by signing into Zoom on the web or by picking the proper options in the meeting.

Basic settings:

1. Require encryption: not sure what this does

2. **Chat:** for livestreaming a class, this should always be **on** while class is in session and no intruders are present. If you want to leave it off until you are sure the room is secure, that is okay. From years of experience, if chat is disabled, things can go horribly wrong with audio in your livestreamed session and the students have not way of telling you if chat is off. Whether you prevent them from saving chat is up to you. They can access chat in the recording.

3. **Private chat**: This should be turned **off** when livestreaming. Otherwise, students can "pass notes" to one another within the session. The receiving student may be annoyed or offended by the note. I see no reason to give students this option.

4. Auto save chat: Sounds like a good option.

5. Sound notification when someone joins or leaves: I think this means everyone in the meeting hears a sound when someone enters or leaves the room. If so, turn this **off**. Sound notifications like these are very annoying to students. In Collaborate, the selected settings only affect what that particular user hears (thus, the notifications are user specific rather than meeting specific). I am not certain how this works in Zoom.

6. Feedback to zoom: another annoyance in my opinion.

7. Display end of meeting survey: use it if you like.

8. Co-host: I would definitely have this **on**. Depending on your setup, you might need to livestream the class from your school account while having a TA or your laptop join the meeting as a co-host. However, note that co-hosts do NOT have the same in meeting controls as host (e.g., co-hosts cannot run breakout groups).

9. **Screen sharing**: This one is subtle. First, if you plan to show PowerPoint, Word, Excel, etc. during class, you must turn this **on**. But, you probably want to be careful with WHO can do what. In most situations, you probably do not want students to share their screens, so pick Host Only for who can share. The next option is who can take sharing control away from someone else. This should always be **Host Only**.

10. **Disable desktop/screen share for users**: Another subtle one. I would leave this one **OFF**. If you turn it on, you can share a word file or a PPT file, but you cannot share both without unsharing the first and start sharing the second. By sharing your whole screen, you can quickly and easily jump between word, PPT, excel, etc.; to do so, this option must be turned OFF. But be careful, sharing your whole screen means your WHOLE screen, so be mindful of whether any sensitive or privileged information is on the screen that you are sharing.

11. Annotation: set who can draw on the screen and whether annotations can be saved. This will depend on if/how annotations are used in your class. I would tend to leave this off. I think if you are sharing from a touch screen monitor and you use the annotation software for the monitor, the annotation will show up on shared content even if you have this turned off. But if annotation is important to you, you probably should practice to see exactly how it works.

12. Whiteboard: if you are likely to use a whiteboard, enable this option and decide if you want to save whiteboard contents.

13. Remote control: apparently, while person A is sharing a screen, person B can request and be granted control over person A's screen if this option is selected. I have not used a function like this in livestreaming, but if it seems useful, turn it on.

14. Nonverbal feedback: If this is selected, participants can send nonverbal feedback and opinions by clicking icons. The icons are raise hand, yes, no, go slower, go faster, thumbs down, thumbs up, clap, a coffee cup (I think means they need a break) and away. This is a personal

choice. I use something like this in Collaborate and really like it, but the functionality may not translate well to Zoom where classes are going to be smaller and most student interactions will be verbal. I require students to use AWAY when they step away so I know not to call on them. I use YES and NO to get a quick sense of the audience without taking the time to launch a formal poll.

15. Reactions: these are similar to nonverbal feedback, but they are emoji's that appear within the participant's video feed. The nonverbal feedback appears in the participant list.

16. Allowed removed participants to rejoin: This is one downside to using both a waiting room and requiring authenticated users. If you mess up and deny a student entry, they generally cannot reenter the waiting room. They are done for the day. To accommodate such situations, leave this option OFF. But that implies you if you detect a Zoombomber, you might have to throw them out several times.

17. Allow participants to rename themselves: I would turn this off for livestreaming. If doing breakout groups or polling, you might have a lot of difficulty matching names to BB IDs if the participants switch names.

18. Hide participant profile pictures: I would likely leave this OFF, but it is a matter of taste. If the participant turns off their webcam or if their webcams are disabled, I can still see their profile picture on the screen. If this is on, you see their name but not profile pictures.

Advanced settings:

19. Report participants to Zoom: I would leave it on.

20. **Breakout room**: I use breakout rooms, so I would always have this **ON**. If you do not, you can have it off. A sub-option allows you to assign participants to breakout rooms when scheduling. Again, Zoom is not BB, so it is not already populated with your students. Also, you cannot assign breakouts with BB IDs because Zoom IDs will not be the same. It appears you need to know in advance which Zoom users will be in a particular session and know in advance their Zoom user name to effectively pre-assign them to groups. But I could be wrong.

21. Remote support: if the student is willing, you can apparently use this feature to control their computer to change a setting, run a program or diagnostic, etc. I doubt you would ever do this while livestreaming. It might be useful in office hours.

22. Closed captioning: don't get excited, Zoom does not close caption. But if you hire someone to close caption in real time, turn this option on and designate the captioner.

23. Save captions: allows captions from (22) above to be saved.

24. Language interpretation: allows you to assign someone the role of interpreter.

25. Far end camera control: Allow a student to control your camera. I would leave this off.

26. Virtual background: handy for hiding what is behind the speaker, but I personally do not like them because sometimes body parts get cut off as part of the backdrop. Sub option allows videos for virtual background. That seems too distracting for a livestream setting.

27. Video filters: I would leave this off. The sort of special effects (animal faces in student videos) seem inappropriate in most business classes.

28. Identify guest participants: This does not seem useful for streaming classes as none of the students are going to have DMSB Zoom accounts.

29. Auto answer: Leave this off. Irrelevant for livestreaming.

30. Default email: I doubt you will be inviting students to class while inside of a Zoom meeting, but if you do, this option control whether you only see Outlook or some other email programs.

31. Use HTML: affects format of invites sent via Outlook plug in.

32. Allow stereo audio: I am unsure how this would improve a student's experience in class.

33. Allow original audio: I am unsure how this would improve a student's experience in class.

34. Select Data Center regions: I think this means if you have students outside the US, you may want to toggle this on and select regions where the students live.

35. Show join from your browser link: This explicitly allows users to use web access to the meeting and avoid downloading the Zoom application. Turning this off seems like a good idea, but in my experience, it is ineffective. I do not know why it is here to be honest.

36. Allow live streaming meetings: this is used to livestream a meeting on Facebook or some other service. I do not see how that relates to livestreaming our classes.

C. Email Notifications: I am not sure how often you would want to get emails on these subjects.

Send when cloud recording is available: you probably want to use this option so you get a reminder when you have a recording in the cloud ready to download.

Other notifications which do not seem that meaningful for livestreaming a class.

D. Other:

1. Blur in iOS: appears to be a security thing for protecting information on your Apple device.

2. Invitation email: let's you send an email invitation in a second language.

3. Schedule privilege: I do not think this applies to faculty at DMSB.

E. ***Recordings***: If you livestream from home using a DMSB provided Zoom account, we require that you save the recording to your hard drive and **not** to the Zoom cloud storage. We recommend you select medium-quality video to save space and upload time.
If you livestream from a first floor classroom using a DMSB provided Zoom account, your only choice is to save the recording to the Zoom cloud. Files saved into the cloud are huge, and the storage available to our Zoom users is small. Thus, you cannot simply post a link to the video in the Zoom cloud. Instead, within 24 hours after class (hopefully sooner to provide timely replays to your students), you must download the video file to your computer. If you livestream from your personal Zoom account, we expect you will run into the same space constraints, so planning to have students access replays stored on the Zoom cloud during the semester seems to be a bad plan.

Uploading to Ensemble: regardless of where you livestream your Zoom class session, you will need to store the session recording on a secure site that students can access without the ability to download. We recommend you create a playlist in Blackboard that links to the session recordings housed in a UofSC storage facility know as Ensemble. With a playlist, after each class, you upload your session recording to Ensemble, and a link to the recording automatically appears in Blackboard for your students to use. A separate document is available from Bob Lipe that describes how to create a playlist and save video files to Ensemble. The document also describes the process by which you request an account on Ensemble; once you have an account, you log into Ensemble.sc.edu with your UofSC ID and password.

Review of recording settings:

1. **Allow local recording**: if you are using a DMSB Zoom account to livestream from home, **you must record to your local drive** for 3 reasons. First, it keeps cloud space open for other faculty recording to the cloud from first floor classrooms. Second, you have the option to save at a lower resolution when saving to your hard drive which will make the file smaller and save you a lot of time on uploading to Ensemble. And third, by saving directly to your hard drive, you eliminate the step in the recording process where you have to download from the cloud to your hard drive. If you are using a DMSB Zoom account to livestream from the first floor, you cannot effectively use local recording.
   A sub-option is to give permission to students to record the session on their hard drive. Doing so would be contrary to policies that only allow students to stream class recordings and not save/download them. This option should be **off**.
   Zoom has a warning for you about local recordings: If the meeting unexpectedly shuts down or if the conversion process is interrupted, the files from a local recording could become corrupted and non-recoverable. Restarting or shutting down your computer, putting the hard disk to sleep, or closing your laptop will interrupt the conversion process.
2. **Cloud recording**: If you are using a DMSB Zoom account to livestream from the first floor, you **must record to the Zoom cloud**. Recording to the hard drive in the classroom is not an option as it takes a while for the recording to be ready after your session ends; another class will be in the room by the time your recording is ready. Zoom documentation specifically warns against using a different cloud service as the "local drive." As mentioned above, a few days of first floor recordings will exhaust the free space in the cloud, so you must download your recording to your hard drive on your office, home, laptop, or personal cloud storage space as soon as possible. You will then need to upload the recording to Ensemble and make it available to students on Blackboard. (Note, posting the video directly to Blackboard will not comply with DMSB security requirements for class session replays; I know of no way to turn off the download option for a video posted directly to BB.)
3. Suboptions for recording – from reading Zoom's help page, it appears that some of these suboptions are available in cloud recording and others are available in local recording:

   When not sharing content, you can pick either active speaker or gallery view to be recorded. The first saves video of the active speaker only, the latter can save up to 25 participant videos.

Shared screen with active speaker records screen contents being shared and video of whoever is talking. This is apparently the only recording with people in it that is available when recording to the cloud.

Gallery view with shared screen shows shared content and some number of attendees (not sure how many). Zoom's help page is confusing; at one place, it says this is only available for local recordings. At another spot, it implies this view can be used with cloud recordings. You will need to experiment to see if this is the best view for your recordings.

Record active speaker, gallery and shared separately records it all. I am not sure what the MP4 file would look like. Zoom's help page implies you have to use Zoom portal to watch such a video, which is inconsistent with migrating the video to Ensemble. I doubt this would work for recording class session in Fall 2020.

Record audio only: this would not comply with DMSB's recording policy for Fall 2020.

Save chat messages: I like to see who said what, so I would save chat if only for my own use. I would not post the chat separate from the video.

Advanced cloud recording settings: Of these, display names might be useful. Optimizing for editing may increase file size. "Save panelist chat" only refers to Webinar Mode sessions, not regular sized sessions like our smaller class meetings.

4. Automatic recording: turning this on might be handy to keep you from forgetting to record.
5. IP Address Control: irrelevant for Fall 2020 as recordings will be move to Ensemble and then deleted from the cloud.
6. Only authenticated users can view cloud recordings: irrelevant because recordings will be moved to Ensemble and deleted from the cloud.
7. Require password to access recording: option to share videos on Zoom cloud should not be enabled. Thus, if sharing is turned off, this setting is probably irrelevant. However, you can turn it on to be safe.
8. Auto delete cloud recordings: you will need to clean up your cloud recordings, but be sure they are loaded on Ensemble before you do so. Auto deletion is kind of scary.
9. Host can delete: I believe this is set to on by DMSB account administrator.
10. Recording disclaimer: Adds a statement to the session that the session is being recorded and by attending, you are consenting to the recording. It then gives students the option to leave the meeting. I do not see this as necessary if you have stated in class and/or syllabus that all DMSB classes will be recorded in Fall 2020.
11. Multiple audio notifications: Apparently this plays a message each time you start and stop the recording. Because you are likely to start and stop recording only once during a class, I would enable this.