JOHNS HOPKINS
UNIVERSITY

Guidelines for Recording with Zoom

August 18, 2020

Zoom is a third-party product that JHU makes available for instructors to use for synchronous video sessions with their students. Instructors can record these sessions for a wide variety of pedagogically valid reasons, but the choice to record a session is a decision made by the instructor. Likewise, the choice to identifiably participate in a recorded session is a decision made by the student.

Like other course content created as part of university activities, these recordings are subject to the Johns Hopkins Intellectual Property Policy. Zoom recordings should be treated as subject to federal student privacy law (FERPA) and the Johns Hopkins University FERPA Policy if students are personally identifiable in the recordings. Please contact your divisional Registrar with any questions.

Zoom is not the recommended tool for creating pre-recorded lectures that can be shared with students. Instead, *Panopto* and *Kaltura* are tools with more options and flexibility for creating asynchronous content. Consult your divisional teaching and learning specialists to see what tools are supported locally.

If an instructor chooses to record Zoom sessions, they should do so in accordance with the following guidelines:

- Use the following Zoom settings (to adjust settings, go to your Zoom in account in your browser):
  - Disable Local Recording. For most instructors, recordings should be kept in the cloud and not downloaded to a local computer. Instructors with accounts that reside on https://jhjhm.zoom.us are subject to HIPAA restrictions; typically, these are faculty/staff who have appointments in SOM, JHHS or affiliates. For these instructors, cloud-based recording is disabled. Graduate student instructors also cannot record to the cloud. These instructors can enable local recording and share via a HIPAA-compliant resource (e.g., OneDrive) if required or using a University video management service (e.g., Panopto, Kaltura).
  - Enable Record active speaker with shared screen
  - Disable Display participants' names in the recording
  - Enable Require password to access shared cloud recordings
  - Enable *Multiple audio notifications of recorded meeting*, which plays an automated message whenever a recording is started, or a participant enters a session that is already being recorded.
  - Enable Recording disclaimer
  - Enable Ask participants for consent when a recording starts
- Notify students beforehand that the Zoom session will be recorded and remind students at the beginning of the class (either orally or using a slide).
- Use the course syllabus to notify students in advance that they may opt-out from identification in the recording by muting their audio, not enabling video, and not typing into the Chat window.
- Instructors should not insist upon student participation that reveals identifying information during the session.
- Students may opt-out from identification in the recording by muting their audio, not enabling video, and not typing in the chat window. In these cases, students should still be considered in attendance and not penalized in any way, and instructors should work with students to determine an alternate method of participation.
- If an instructor insists upon participation that reveals identifying information during class (either by audio, video, or chat), then the session should not be recorded.
- Unless the recording is subject to a litigation hold as directed by the Office of the Vice President and General Counsel, instructors must manually delete all recordings by 120 days after the last day of the

course (however, earlier deletion is preferable unless there is a reason to keep the recordings until the deadline).

Using Zoom in Courses Discussing Politically Sensitive Topics with Students in Vulnerable Locations

It is also important to be mindful of students taking courses in countries where academic freedom and freedom of expression are restricted by the government. Classes which engage in critical discussions of authoritarian states might pose a risk to students through surveillance or censorship. Zoom is increasing its encryption of live sessions to address these concerns; however, no technical solution can eliminate risk. Below are recommendations to minimize risk for students in courses discussing politically sensitive content.

- Consult with students about their concerns engaging in conversations or sharing course work subject to surveillance. Provide accommodations as appropriate.
- Do not record and share course conversations with students in or from vulnerable locations. Tell other students to not record and share conversations with their peers.
- Allow students to anonymously participate in discussions without identifying themselves or turning on their video.
- Consider alternative ways for students to share their ideas, such as scheduling separate office hours to discuss course content or using alternative, encrypted communication channels like Signal.

For more information on this topic, please consult the Association for Asian Studies *Statement Regarding Remote Teaching, Online Scholarship, Safety, and Academic Freedom*.