Guidelines for Recording with Zoom

September 11, 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 in which students' participation may be captured, they should do so in accordance with the following guidelines to minimize recording identifiable student participation as required by FERPA policy:

- Use the following Zoom settings. To adjust settings, go to your Zoom account in your browser (JHU Zoom Help - https://uis.jhu.edu/zoom/):
    - Disable the "record gallery view" option and enable the "record active speaker with shared screen" option in order to only record those who speak during the session. Students can choose to not show their video if they do not want it captured when they speak.
    - Disable the option for "display of participants' names in the recording." Names will still be viewable to participants during the meeting, but will not be included in the recording.
    - Enable the "require password to access shared cloud recordings" option.
- 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.
- Notify students beforehand that Zoom sessions will be recorded – i.e. in the course syllabus. Similarly notify students beforehand that they may opt-out from identification in the recording by muting their audio, not enabling video, and not typing into the chat window. Remind students at the beginning of the class (either orally or using a slide) that the session will be recorded, and their options for opting-out of identification in the recording. In addition, all participants will automatically be notified of and be prompted to consent to the recording in Zoom.
- Instructors should not insist upon student participation that reveals identifying information during the session.
- Consider offering to pause the recording when students participate to avoid capturing their audio and video. For instructors who desire to make recordings available to other classes/cohorts, avoiding capture of student audio and video during class participation will allow the instructor to share the recording without first obtaining student consent prior to sharing a class recording. (See additional information below.)
- 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.

Office of the Provost • Stephen J. Gange, PhD • Executive Vice Provost for Academic Affairs
253 Garland Hall, 3400 N Charles St. • Baltimore, Maryland 21218 • Tel: 410-516-5610 • sgange@jhu.edu

- Delete recordings of identifiable student participation, including complementary files (e.g. transcript, chat logs) and Zoom recordings hosted on other platforms (e.g. Panopto, Kaltura), as soon as your obligations to your students allow. Deletion by 120 days after the last day of the course is recommended unless the recording is subject to a litigation hold as directed by the Office of the Vice President and General Counsel. Until it is deleted, any recording of identifiable student participation should be treated as a student record subject to FERPA.
- Disable the "local recording" option. 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).
- Access to class recordings must be limited to students in the class for educational review purposes. Faculty should include a statement on the syllabus or communicate in an equivalent method to all students in the class, "Class meetings recorded by the instructor may be shared with students in the class for instructional purposes related to this class. Students are not permitted to copy or share the recording with others." For any disclosure beyond the class or for other purposes, identifiable student information must be removed or students who are identifiable must provide written consent prior to disclosure.

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*.