Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Instructions for Using the Zoom Video Conference System of 30 October 2020

The previously issued Instructions for Using the Zoom Video Conference System of 19 June 2020 and the Addition to the Instructions on Using Zoom (Issued on 19 June 2020) are superseded by these instructions.

Digital events and meetings have been indispensable during the coronavirus pandemic. These digital solutions should aim to offer not only the large events such as lectures, but also the smaller discussions, and even job interviews, that form part of the University's daily business securely and without disruption. The video conference system Zoom offers these possibilities while meeting the technical conditions and observing the instructions issued by the University.

For this purpose, the Regional Computing Center (RRZ) has created its own server capacities, whereby it can move a conference from Zoom's own servers to host it exclusively on Universität Hamburg's servers. Additionally, using Zoom in accordance with data protection policies requires compliance with specific codes of conduct.

Therefore, these instructions contain guidelines for using Zoom to which all Universität Hamburg employees must adhere. For tips on following the guidelines below and using Zoom technology, see

https://www.rrz.uni-hamburg.de/zoom.

1. Exclusive use of Universität Hamburg's Zoom services

Zoom may only be used through Universtiät Hamburg's Zoom services, which you can access at http://uni-hamburg.zoom.us. This is the only way to ensure that communication takes place via the server operated by the RRZ and that data remains confidential. It also ensures that users setting up a meeting use their uni username, thereby working within the University's authentication infrastructure at the RRZ. You are not expressly prohibited from taking part in video conferences hosted by colleagues at other institutions or outside Universität Hamburg. However, depending on the data protection requirements for specific information and the type of video conference, caution is advised: not everyone requires such stringent data protection measures or confidentiality policies as Universität Hamburg.

2. Limiting the number of participants

To further ensure confidentiality with regard to both word and image at events and conferences and to prevent disruptions or attacks ("Zoombombing"), the number of participants should be limited to invitees only. Therefore, the event host must always set up the respective meeting with password protection and only send the password with the invitation in order to ensure that only those authorized participate. It is not permitted to publish the password on the website.

Participants should be informed that passing on login details is strictly forbidden.

Admitting unauthorized third parties may result in the outflow of personal data—something the University must avoid at all costs.

3. Recording events, lectures, and video conferences

Recordings can only be made in accordance with data protection regulations. Therefore, the only Zoom meetings that are allowed to be recorded are webinars, thus ensuring only the lecturer is filmed. The lecturer must first register the webinar on SharePoint, and all speakers who will be seen in the recording must give their consent on the corresponding consent page. Individual lecturers employed by Universität Hamburg can do this themselves. Lecturers not employed by Universität Hamburg must give consent as a PDF, which is to be uploaded by the lecturer who registered the webinar. Use the following link to go to the registration and consent page in SharePoint:

https://uhh.de/einwilligung-aufzeichnung.

Non-webinar events, lectures, or discussions may not be recorded.

Be sure to observe the following additional guidelines for recording webinars:

a. Questions only via the chat and Q&A function

   Use the invitation email to inform students and participants in advance that they will not be able to speak and that they can only ask questions and have them answered via the chat and Q&A functions. The chat session will not be recorded.

b. Teaching participants in hybrid in-person courses

If participants physically attend an event in the lecture room, inform them at the beginning of the event that questions asked aloud may be heard on the recording and that being aware of this possibility constitutes consent. Alternatively, participants attending in person can also ask questions using the chat and Q&A functions. It is assumed that participants attending in person will bring suitable mobile devices and log in as webinar participants.

c. Do not allow additional speakers

Lecturers and event hosts are not authorized to assign the role of discussion participant to anyone else who is not a designated speaker and has not given their consent to being recording in SharePoint.

d. Setting up a webinar

Apply to use the webinar function via the following link: https://uhh.de/zoom-webinar. As host, log in at https://uni-hamburg.zoom.us, select the webinar function from the side bar, and then enter the basic parameters that were registered as event data in SharePoint.

Do not activate the "Registration" function. You must use a webinar code, and select the option "Questions and Answers" under "Webinar Options."

If a participant tries to log in via a mobile device, Zoom currently asks for a name and email address. This cannot be issued at present. **Participants are informed in the invitation and in the notes on the RRZ's website that any name and the email address "a@b.de" can be entered when using Zoom with a mobile device.** As soon as Zoom resolves this problem, you will no longer receive this prompt.

An email containing the invitation will then be sent to the participants. Please note, as mentioned above, that online participants can only ask questions via chat or the Q&A function. In-person participants are informed about the recording and advised that persons outside of those present may hear any questions or feedback spoken out loud. Those who do not want to be recorded can also ask questions via chat or the Q&A function. It is assumed that participants attending in person will bring suitable mobile devices and log in as webinar participants.

4. Deleting minutes, chats, etc.

At the end of a video conference, chats and minutes will be deleted automatically. There are no such minutes or records for in-person events; thus, this should not pose a problem. Deletion is required to ensure data protection.

5. Turning off the video function for participants

The systems being used allow participants to decide for themselves whether they wish to be seen or heard. If it is not necessary for participants to be seen, they should be informed at the beginning of the session that the camera on their own device can be turned off. This makes good sense from a data protection standpoint, and it minimizes the broadband used for the event.

6. Names of participants

Zoom enables participants to use pseudonyms instead of their real names. Because this data is sent to Zoom, participants are instructed not to provide their real names if they do not wish to do so. If it is important to determine identity, a pseudonym (e.g., a student ID number or staff code) should be used.

7. Sharing the screen

The host of a given session can share individual windows on their screen with all participants and thus provide access to the content on their PC. The host must therefore make sure that any shared windows do not contain the personal data of a third party. We recommend only sharing the window of the application that is intended for joint viewing (e.g., PowerPoint). Each meeting participant must ensure that they do not reveal the personal data of third parties (e.g., via an open email box).

8. Muting other participants

The host can mute the microphones of other participants. This is a good way of preventing background noise. It also protects participants from inadvertently revealing the personal data of third parties. Thus, the host should make regular use of this function.

9. Invitation

When you send invitations to a conference, you should advise that invitees can take part using a pseudonym and that access details are not to be shared with others.

Univ.-Prof. Dr. Dr. h.c. Dieter Lenzen

Hamburg, 30 October 2020