Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Instructions for Using the Zoom Videoconference System of 30 July 2021

The previously issued Instructions for Using the Zoom Videoconference System of 30 October 2020 is superseded by these instructions.

Digital events and meetings have been indispensable during the coronavirus pandemic. These digital solutions should aim to offer not only online examinations and 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 videoconference 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 Universität Hamburg's Zoom services, which you can access at http://uni-hamburg.zoom.us. You must install the Zoom client software on your end device, you are not able to use the service through a web browser. The only way to ensure that communication is carried out in compliance with data protection regulations and that data remains confidential is to use the server operated by the RRZ in Universität Hamburg. 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 videoconferences hosted by colleagues at other institutions or outside Universität Hamburg. However, depending on the data protection requirements for specific information and

the type of videoconference, caution is advised: not everyone requires such stringent data protection measures or confidentiality policies as Universität Hamburg.

2. Setting up a meeting

a. Topic or title

When setting up a meeting, the topic or title of the meeting must be kept generic (e.g., "Zoom meeting"), as this information is transmitted to the Zoom company. When inviting participants (e.g., via Outlook), the actual topic or title of the meeting can be used.

b. Invitation text

As part of the invitation, the participants in a conference must be advised that they may participate under a pseudonym, that they are not permitted to share contact data, and of their rights under Articles 12–21 of the General Data Protection Regulation (GDPR). Invitations sent via the Zoom client will automatically include a relevant notice (https://uhh.de/einladung-zoom-meeting, in German), which may not be shortened or deleted.

c. 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 teaching

Teaching can only be recorded in accordance with data protection regulations. Therefore, teaching sessions must be recorded as webinars with only the lecturer visible.

Non-webinar events, lectures, or discussions may not be recorded. Recording is not permitted outside of teaching.

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 in advance and at the beginning of the lecture that questions from those physically present may only be asked via the Chat and Q&A function, for which they must log into the webinar on a mobile device.

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.

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. If participants physically attend an event in the lecture room, they must be informed as stated above, that participants who are physically present may only ask questions via the Chat or Q&A function for which they must log into the webinar on a mobile device.

4. Deleting minutes, chats, etc.

At the end of a videoconference, 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

In principle, the systems being used allow participants to decide for themselves whether they wish to be seen and/or heard. This does not apply when the purpose of the meeting requires both video and audio (e.g., online examinations, job interviews).

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. Rather, unless the clear text provision of a name is required, a pseudonym (e.g., a student ID number or staff code) should be used.

7. Authenticating participants in online examinations

If participants need to be identified for online examinations, this must be carried out by presenting official photo identification (e.g., identify card, passport). Where multiple persons are

involved, this authentication should take place individually in a separate room (breakout room).

8. 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).

9. 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.

Univ.-Prof. Dr. Dr. h.c. Dieter Lenzen
Hamburg, 30 July 2021