Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Instructions for Using the Zoom Video Conference System 19 June 2020

Digital events and meetings have been indispensable during the coronavirus pandemic. The goal should be to offer events such as lectures, discussions, and even interviews that form part of the University's daily business securely and without disruption. The video conference system Zoom makes this possible while meeting the technical conditions and allowing users to observe the instructions issued by the University.

In the last few weeks, the Regional Computing Center (RRZ) has created its own server capacities, whereby it can pull the conference in question from Zoom's own servers and offer 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

It is permissible to use Zoom only by using Universität 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. This means that you need to send a password with your invitation. This ensures that only those who have been authorized to do so can take part.

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. Prohibition on recording events, lectures, and video conferences

Recording an event, lecture, or other type of video conference is strictly prohibited.

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 their screen with all participants and thus provide access to the content on their PC. The host must therefore make sure that the shared screen does not contain the personal data of a third party. It is a good idea to share only the data required and to close all other windows; alternatively, you can open a new window or screen. It may be best to limit the number of windows you share. You must ensure that you 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 note that invitees can take part using a pseudonym.

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

Hamburg, 19 June 2020