As you will know, on-campus teaching activities will not take place until further notice. These have now been transferred to online scenarios, where synchronous interaction (like tutor group meetings, online lectures) can be realised by means of [Zoom](https://zoom.us/).

Zoom is a cloud-based video conferencing service, that you can use to virtually meet with others - either by video or audio-only or both. Zoom can be compared with Skype, but has several extra functionalities that support online teaching, learning and collaboration.

Some staff and students expressed their concerns about Zoom privacy and security issues. However, many issues can be linked to ignorant, unsafe or basically wrong use of this application by a user. The UM obtained a campus license (until further notice only available for staff members) a few weeks ago. This campus license already enables extra Zoom platform parameters for security and privacy. For instance, the recording of Zoom sessions has been disabled within the license.

Our faculty staff has been informed as well, how to set up and host Zoom sessions in the best possible way. This includes the latest security and safety recommendations published on the [Zoom blog](https://blog.zoom.us/wordpress/2020/03/20/keep-uninvited-guests-out-of-your-zoom-event/). Next to this, recommendations from [universities](https://security.berkeley.edu/resources/cybersecurity-and-covid-19/settings-preventing-zoom-bombing) who already use Zoom for a while, have been a very useful source.

Still, bullet proof privacy and security are only possible, if all students will act according to the following Zoom rules.

1. Never share Zoom meeting details (the meeting link, ID, password) with others, nor share these details on open platforms. Zoom bombings and trolling happened because meeting details were (publicly) shared.
2. Never sign in to Zoom with your Facebook or Google account. Zoom offers that opportunity on the login screen, to make it easier for people to join. However, when you sign in with Facebook or Google, you are opening the door to these platforms to harvest personal data. As a matter of fact: such data harvesting occurs within every application, whenever someone signs into it with a Facebook or Google account. Needless to say, [the same kind of data mining will happen when using Facebook or Google applications](https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy).
3. You can join a Zoom meeting without the need to login. Nevertheless, the UM is asking all students to create a [free Zoom account](https://zoom.us/) - by means of the student email address and full name. [The university is busy extending the campus license to students as well](https://www.maastrichtuniversity.nl/education/online-education-um/students). The moment that this will be the case, the UM-email-based free Zoom account can be linked to the campus license.
4. Students must be aware, that whenever they organise Zoom sessions themselves, as a host they have to safeguard the same [security and privacy settings](https://blog.zoom.us/wordpress/2020/03/20/keep-uninvited-guests-out-of-your-zoom-event/) as lecturers do.
5. A lecturer can set the microphone for all students on mute by default for a Zoom session. Additionally, the sharing of screens by students might be disabled too. Though these settings can be altered during a session, they are basically there to ensure a safe and well-organised meeting.
6. We recommend that students will already enter a Zoom meeting or its ‘Waiting Room’ 5 minutes before the start, to check if their equipment (microphone, webcam, headset/headphone, overall device settings) is working well. If you have a headset/headphone, then please use it. It can prevent that surrounding noises coming from your location, will become a disturbing factor for the other participants and yourself.

When we will all stick to these rules, nothing will stand in the way of safe and successful meetings!