

Privacy & Corona: Appendix for teachers

Online teaching and the use of new tools bring with them new privacy concerns. This brief overview will explain the basics of what you need to know as a teacher under these new circumstances.

Using new tools

Please be aware that due to privacy regulations, you can only use tools that have signed a data processing agreement (DPA) with Leiden University. We do not support the use of tools that have not signed a processing agreement, nor can we guarantee their safety. If you are unsure whether a tool has been cleared for use, please contact privacysupport@hum.leidenuniv.nl.

Online classes & webcams

Due to privacy regulations, we recommend you use Kaltura for your online classes. If you must record your classes please make sure of the following:

- ▶ You have no other way of providing your course.
- ▶ The course cannot be replaced with a Kaltura capture video.
- ▶ Students are warned that they will be recorded, either in writing or in person, before the recording starts.
- ▶ You stop the recording after your class is finished.

Though it may feel more natural to be able to see your students during an online class, bear in mind that students are allowed to turn off their cameras. Allow students to do so unless there is a concrete reason they must keep them on (e.g. during a presentation). Provide a clear explanation of if and when you want your students to turn their camera on.

Unauthorised recording or image capturing of online teaching using third party software is not allowed. Be aware that if you record your lecture on Kaltura Live Room, your students' names and/or camera feed will be visible unless they turn their cameras off. You will need to ask for individual consent if sharing this information. You can avoid this by asking students to turn off all webcams. Please bear in mind copyright and licensing restriction apply when making video courses.

Online quizzes can be made in MS Teams through the Forms app. You can turn off the visibility of participant names and email addresses; please do so if you do not need to see this information.

Video Conferencing

Please use MS Teams for all meetings and/or one-on-one communication when possible, as Leiden University has a Data Processing agreement with Microsoft. Zoom and other unsupported tools should be strictly avoided unless it has been specifically stated a DPA has been signed by the companies in question.

Unauthorised recording or image capturing of online meetings with third party software is not allowed.

Be aware that if you record meetings or lectures on MS Teams, participants' names and/or their camera feed will be visible unless they turn their cameras off.

Please also note MS Teams currently has an issue where any recordings made during a meeting will be available to download for the entire Team site. The only currently known workaround is to delete the Team site after a meeting has concluded.

Brightspace:

Be mindful of how you communicate grades to students. Placing a list of grades for all your students to see, for example, is considered a breach of privacy. Use the "Grades" function in Brightspace to post grades to your students; you can find more information on how to properly configure Grades [here](#).

Online exam monitoring (proctoring)

Exams during the Covid-19 pandemic should be adapted so they can be administered to students remotely. Different options are available for this purpose, such as creating take-home exams or administering open book exams.

If your course does not lend itself to adapting exams, you may want to opt for a proctored exam. During a proctored exam, your students and their screens will be monitored by a company contracted by Leiden University.

- ▶ Students will not have to show their social security number/BSN during the monitoring progress, as this considered sensitive data.
- ▶ If your students have privacy-related concerns regarding a proctored exam, please request that they address these concerns to the Data Protection Officer (Functionaris Gegevensbescherming) for now. The contact person may be subject to change. The DPO can be reached through privacy@bb.leidenuniv.nl

Data security

Working remotely offers an additional set of challenges when it comes to your security. Please take the following steps to ensure your workplace is secure when working from home:

- ▷ Make sure your operating system has been updated to the latest version;
- ▷ Install antivirus software and ensure Windows Security features are up-to-date and enabled;
- ▷ Use the university's remote workplace whenever possible;
- ▷ Ensure your Wi-Fi network is secure, and use EduVPN or another secure VPN of your choice;
- ▷ Do not use unauthorised file transfer tools, such as Google Transfer. Use SURF's FileSender for all your file transfers, or Surfdrive for sharing files with a group;
- ▷ Avoid alternative email browsers or applications;