AUTORITEIT
PERSOONSGEGEVENS

Online voice and video calls & privacy

Recommendations for educational institutions

As an educational institution, do you use a system for online voice and video calls? Or do you have plans to do so? If so, take the following points into account to ensure that you protect the privacy of your pupils or students and your staff. A checklist is provided at the end.

Getting started

Purpose and legal basis

- Consider why exactly you want to use online voice and video calls and make sure you can justify your decision.
- Determine the legal basis under the GDPR for your use of online voice and video calls.
- Note: you are not permitted in any circumstances to use the collected data for any purpose other than this predetermined purpose.

Necessity (of recording the calls)

- Check if it is necessary for students or pupils and teachers to be visible on screen in order to achieve your purpose.
- Will you be recording the lesson or lecture, for instance so it can be viewed again later? If you are, in principle no pupils or students may be visible in the recording. That is why you need to specify in advance when the recording will start, so your pupils or students will know when to turn off their microphone and camera.
- You are not allowed to make recordings that display pupils or students without good reason, and only in exceptional situations. If you want to do so, you must be able to set out why this is necessary, and explain this clearly to your pupils or students in advance.
- Use the application's default settings to protect privacy as much as possible.

DPIA

- Perform a DPIA before making online voice and video calls. This is often mandatory.
- If possible, also involve pupils/students and teachers.
- Periodically check whether you need to review the DPIA, for example if coronavirus measures are relaxed.

Cooperation

- Involve the DPO in good time if planning to use online voice and video calls. Informing the DPO afterwards about the choices that were made is not sufficient.
- Discuss solutions for remote teaching with stakeholders, such as the student council and the participation council.
- Collaborate with other school boards and/or umbrella organisations. Share knowledge and exchange experiences. Join forces with other organisations to approach major players in the market.

Procurement

Selecting a supplier

- You must choose a software supplier that complies with privacy laws.
- Set requirements for how the personal data of your pupils/students and staff, including (vulnerable) children, is used. In any case, ensure that any data that is not necessary is deleted immediately.

Entering into a data processing agreement

- Enter into a data processing agreement with the supplier.
- Ensure that the agreement meets the requirements of the GDPR, at the very least.
- Particularly in case of suppliers outside the EEA, make sure that appropriate safeguards are in place.

Preparation and instructions

Drafting policies

- Draw up an institution-wide policy on using online voice and video calling apps or software programs. At a minimum, it should state when online voice and video calls can be used, and the describe the resources and methods used to process personal data (such as retention periods, security and access to the data).
- Translate this policy into concrete guidelines and instructions for teachers and pupils/students.

Providing information and instruction

- Inform pupils, students and parents about what happens to their data, in language they can understand.
- Inform pupils, students and parents about their privacy rights.
- Instruct your pupils or students to keep personal items out of sight. Is there too much sensitive, personal information visible during online video calls? If there is, ask the pupil or student to turn off their camera, or make sure that you can turn the camera off yourself to protect the pupil/student.

Rights of students, pupils and parents

- Set up a process to allow students, pupils and parents to exercise their rights – for example, if a student or pupil requests access to recordings.

Being prepared for incidents

- Keep in mind that it is impossible to completely rule out data breaches or other incidents, no matter how well you have set everything up. Be prepared for this.
- Discuss with pupils/students and teachers what can go wrong and what to do in these situations in order to minimise the potential impact.

Checklist for online voice and video calls

Getting started
□ determine purpose and legal basis
□ determine necessity
□ perform a DPIA
□ seek cooperation with others
Procurement
□ select a supplier
□ draft a data processing agreement
Preparation and instructions
□ draft policies
□ provide information and instruction
□ rights of students, pupils and parents
□ be prepared for incidents