AUTORITEIT
PERSOONSGEGEVENS

Corona & privacy

Tips voor het onderwijs

Tijdens de coronacrisis krijgt een groot deel van alle leerlingen en studenten in Nederland digitaal thuisonderwijs. Dit gebeurt onder meer via beeldbellen en proctoring (digitale surveillance bij tentamens of toetsen).

Het gebruik van deze digitale middelen kan grote impact hebben op de privacy van leerlingen, studenten en docenten. De Autoriteit Persoonsgegevens (AP) geeft daarom tips aan onderwijsinstellingen die beeldbellen en proctoring (willen) inzetten.

Beeldbellen

Gebruikt u als onderwijsinstelling een systeem voor beeldbellen? Of wilt u dat gaan doen? Let dan op de volgende punten:

1. Maak gebruik van de Keuzehulp videobel-apps van de AP en de website lesopafstand.nl, samengesteld door onder meer het ministerie van OCW en branchevereniging.
2. Kiest u voor een softwareleverancier, dan bent u verplicht om er een te kiezen die voldoet aan de privacywetgeving. U moet eisen stellen aan het gebruik van data van uw leerlingen, studenten en personeel, waaronder (kwetsbare) kinderen. Leg in dit geval de nadruk op het direct wissen van gegevens die niet noodzakelijk zijn.
3. Informeer leerlingen, studenten en ouders over wat er met hun gegevens gebeurt, in voor hen begrijpelijke taal.
4. Kies een oplossing in samenwerking met de medezeggenschapsraad. Belangrijk is dat docenten, leerlingen en ook ouders betrokken zijn bij deze keuzes.
5. Werk samen met andere schoolbesturen. Deel kennis en wissel ervaringen uit. Trek samen op richting grote spelers op de markt.
6. Bedenk dat u verantwoordelijk bent voor de manier waarop het beeldbellen plaatsvindt. U kunt bijvoorbeeld uw leerlingen instrueren om persoonlijke zaken buiten beeld te laten.
7. Komt er te veel gevoelige, persoonlijke informatie in beeld? Vraag aan de leerling om de camera uit te zetten of zorg dat u de camera kunt uitzetten om de leerling te beschermen.
8. Bedenk dat een datalek of ander incident nooit helemaal uit te sluiten valt, hoe goed u alles ook ingericht heeft. Wees hierop voorbereid. Bespreek met leerlingen en docenten wat er zoal kan misgaan en wat te doen in deze situaties.

AUTORITEIT
PERSOONSGEGEVENS

Proctoring

Maakt u als onderwijsinstelling gebruik van proctoring (digitale surveillance)? Of wilt u dat gaan doen? Let dan op de volgende punten:

1. Ga na of proctoring noodzakelijk is. Kijk eerst of er een minder ingrijpende methode van examinering mogelijk is. Bijvoorbeeld door leerlingen of studenten een werkstuk of essay te laten inleveren. In veel gevallen is het mogelijk om een oplossing te kiezen die minder inbreuk maakt op de privacy van uw leerlingen of studenten.
2. Is het echt noodzakelijk? Zorg dan in ieder geval dat de inbreuk op de privacy zo klein mogelijk is. Bijvoorbeeld door toetsen of tentamens samen te voegen, zodat u het aantal momenten van proctoring beperkt. En door te kiezen voor de minst ingrijpende vorm van proctoring. In veel gevallen is bijvoorbeeld eyetracking een te zwaar middel.
3. U bent verplicht een leverancier te kiezen die voldoet aan de privacywetgeving. U moet eisen stellen aan het gebruik van data van uw leerlingen, studenten en personeel door deze leverancier. Selecteer de aanbieder van het systeem zorgvuldig. Belangrijk is dat alle gegevens direct gewist worden als u deze niet meer nodig heeft. Verzeker u ervan dat de (software)aanbieder deze gegevens gelijk wist zodra dat kan.
4. Bespreek oplossingen voor het afleggen van examens in samenwerking met de studentenraad.
5. Gebruik de gegevens niet voor andere doeleinden dan examenfraude bestrijden.
6. Informeer uw leerlingen of studenten in begrijpelijke taal over wat er met hun gegevens gebeurt.
7. Instrueer uw leerlingen of studenten over proctoring. Studenten moeten weten hoe zij op een zo privacyvriendelijk mogelijke manier hun toets of tentamen kunnen afleggen.
8. Bedenk dat een datalek of ander incident nooit helemaal uit te sluiten valt, hoe goed u alles ook ingericht heeft. Wees hierop voorbereid.