

Veilig omgaan met persoonsgegevens?

Dat doe je zo!

Wat betekent de Europese privacywet (Algemene verordening persoonsgegevens; de AVG) in de dagelijkse praktijk voor jou en je collega's? De belangrijkste privacyregels vind je hieronder. Werk je op deze manier? Dan ben je goed bezig!

Waar en hoe bewaar ik persoonsgegevens?



Bewaar gegevens digitaal

Bewaar persoonsgegevens zoveel mogelijk digitaal op de afgesproken (veilige) bewaarplaatsen.



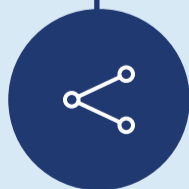
Werk zorgvuldig en professioneel

Moet je gegevens over een persoon vastleggen? Zorg dan voor een zorgvuldige en professionele omschrijving.



Gebruik een veilige computer

Gebruik voor de verwerking van leerlinggegevens bij voorkeur een computer van school. Kan dat niet en moet je toch vanaf een privé computer werken? Zorg er dan voor dat deze goed beveiligd is.



Deel niet zomaar persoonsgegevens

Vraagt iemand jou om persoonsgegevens van een ander? Ga dan eerst na of dit nodig is en welke afspraken hierover binnen je school gemaakt zijn.

Hoe en wat communiceer ik online?



Foto- en filmopnames delen

Wil je foto's of video's waarop leerlingen of collega's te zien zijn delen via bijvoorbeeld social media of de website? Controleer dan eerst of hiervoor toestemming is gegeven, schriftelijk dan wel online. Zo niet, dan mag je die foto's of video's niet delen.



Mail beveiligd

Het is veiliger om een link naar documenten te delen dan om deze als bijlage te versturen via e-mail. Maak voor gevoelige en bijzondere persoonsgegevens gebruik van een oplossing voor beveiligd mailen.



Pas op voor phishing en spoofing

Klik alleen op linkjes en open alleen bijlagen in e-mails van betrouwbare afzenders. Vul nooit je inloggegevens in op een website die je normaal hiervoor niet gebruikt en geef deze ook niet desgevraagd door aan iemand.



Gebruik BCC

Stuur je een bericht naar een (grote) groep mensen, die niet allemaal van je eigen organisatie zijn? Zet de e-mailadressen dan altijd in de BCC-regel.

Hoe houd ik onbevoegden op afstand?



Beveilig je computer en werkomgeving

Vergrendel je computer of meld je af als je je werkplek verlaat. Zorg ervoor dat er op je bureau en bij de printer geen gevoelige informatie ligt. En bewaar laptops of tablets op een veilige plek.



Pas op met meekijkers en -luisteraars

Zet je digibord op freeze als je wachtwoorden intoetst of persoonsgegevens in beeld staan. En zorg dat niemand meekijkt als jij je wachtwoord intoetst of meeluistert bij vertrouwelijke (telefonische) gesprekken.



Kies een sterk wachtwoord

Laat je wachtwoorden van digitale (administratie) systemen met persoonsgegevens niet onthouden door je internetbrowser. Kies een sterk wachtwoord, schrijf het niet op en deel het niet met collega's of anderen.



Gaat het mis? Meld het meteen!

Als je persoonsgegevens kwijt raakt, onbevoegden er toegang tot hebben gekregen, of als je gegevens niet meer toegankelijk zijn, meld dit dan meteen bij je leidinggevende. Het kan een datalek zijn.