

Werkplek

- [Vergrendel](#) je scherm bij het verlaten van je computer door toets combinatie Ctrl-Alt-DEL en Enter of Windows toets  en L
- Zorg dat leerlingen niet op je scherm kunnen [meekijken](#) terwijl je aan het werk bent
- Houd je [wachtwoorden persoonlijk](#) en deel deze niet met anderen
- Controleer een [veilige verbinding](#) met websites waarop je inlogt: HttpS:// i.p.v. http://
- Print veilig als anderen bij jouw printer kunnen, kies beveiligde afdruk – pincode

Data integriteit

Wees **bewust** dat je werkt met persoonsgegevens die van leerlingen, medewerkers, of van jezelf. Persoonsgegevens zijn gegevens zoals NAW, BSN en foto's. Bijzondere persoonsgegevens zijn gegevens die gaan over de persoon zelf en die zo gevoelig zijn dat de verwerking ervan iemands privacy ernstig kan schaden, bijvoorbeeld:

- [Gegevenslocaties](#): sla persoonsgegevens zorgvuldig op in de systemen van de school zoals Office365, OneDrive, schooladministratie zoals Magister, Youforce, etc.) en NIET op usb, privé apparaten of smartphones
- [Surf zorgvuldig](#), klik niet klakkeloos op linkjes
- Klik in de mail niet op [onbetrouwbare](#) bijlagen en linkjes
- [Deel zorgvuldig](#) gegevens en bestanden met collega's
- Deel persoonsgegevens zorgvuldig met externen, controleer of er een [verwerkingsovereenkomst](#) is afgesloten
- Gebruik voor het delen van bestanden met persoonsgegevens [delen](#) (link naar een document bijvoegen i.p.v. een kopie zie [handleiding SharePoint](#)) i.p.v. van een kopie toe te voegen als een bijlage
- Beveilig bestanden met persoonsgegevens met een [wachtwoord](#) en verstuur het wachtwoord in een aparte mail of bel dit door
- [Sla bijzondere persoonsgegevens alleen](#) op in schooladministratiesystemen zoals Magister, SOM en Presentis
- [Wissel alleen BSN](#) uit met andere onderwijsinstellingen
- Bij inloggen in schoolsystemen is [tweede authenticatie](#) verplicht indien je buiten de school werkt. Deze tweede authenticatie wordt na de zomervakantie 2018 ingevoerd.

Beveiligingsincidenten

- Een [beveiligingsincident](#) is een gebeurtenis waarbij de mogelijkheid bestaat dat de beschikbaarheid, integriteit of vertrouwelijkheid van informatie of informatie verwerkende systemen in gevaar is of kan komen
- Een [datalek](#) is een beveiligingsincident, waarbij gegevens verloren zijn geraakt of onrechtmatig kunnen worden bewerkt (opgeslagen, aangepast, verzonden, gedeeld, enz.)
- Alle beveiligingsincidenten, dus ook datalekken, dienen te worden geregistreerd via het e-mail adres datalek@achterhoekvo.nl door de IBP verantwoordelijke of functionaris gegevensbescherming.
- Een medewerker kan ook zelfstandig een incident melden bij datalek@achterhoekvo.nl of fg@achterhoekvo.nl.

- De functionaris gegevensbescherming zorgt voor het afhandelen van incidenten met een vertrouwelijk karakter.
- Een verdwenen leerling- of personeelsdossier op [papier](#) is ook een beveiligingsincident en dient ook te worden geregistreerd
- **Datalekken moeten door de functionaris gegevensbescherming worden gemeld bij de Autoriteit Persoonsgegevens**

Bewaartermijnen

- Leg geen [archief](#) aan (b.v. op het netwerk) met persoonsgegevens die niet langer noodzakelijk zijn voor het verwerkingsdoel
- Het uitgangspunt blijft dat [bijzondere persoonsgegevens](#) niet langer bewaard mogen worden dan noodzakelijk voor het doel van de verwerking. Voor bijzondere persoonsgegevens van leerlingen is dit 5 jaar en voor bijzondere persoonsgegevens van medewerkers is dit 7 jaar
- Voor sommige gegevens gelden wettelijke bewaartermijnen. Zo moeten gegevens die fiscaal van belang zijn 7 jaar bewaard blijven. Wanneer er geen wettelijke bewaartermijn van toepassing is geldt over het algemeen een bewaartermijn van 2 jaar. Zijn de gegevens eerder niet meer nodig? Dan moeten ze direct verwijderd worden.'
- [Recht op vergetelheid](#): collega's, leerlingen en ouders hebben het recht om de school te vragen om bijzondere persoonsgegevens uit systemen te verwijderen. Dit moet door de school óók worden gemeld aan organisaties die deze gegevens hebben verwerkt
- [NAW](#) gegevens mogen wel bewaard blijven

Social media

- Maak duidelijk of je op persoonlijke titel of namens Achterhoek VO publiceert
- [Publiceer](#) geen vertrouwelijke informatie op social media
- Ga niet in [discussie](#) met een leerling of ouder op social media
- Medewerkers van Achterhoek VO zijn [persoonlijk verantwoordelijk](#) voor wat zij publiceren, tenzij duidelijk is aangegeven dat er namens Achterhoek VO wordt gesproken
- Bij twijfel over een publicatie of over de raakvlakken met (het beleid van) Achterhoek VO zoeken medewerkers van Achterhoek VO vóór publicatie contact met een leidinggevende
- Leden van het bestuur, rectoren, directeuren en leidinggevenden zijn altijd vertegenwoordiger van Achterhoek VO, ook als zij als zij op persoonlijke titel spreken en b.v. een privémening verkondigen

Nieuwe privacywetgeving vanaf 25 mei 2018

De AVG in een notendop



Op basis hiervan mag je persoonsgegevens verzamelen

De grondslag



Toestemming
van de gebruiker



Vitale belangen



Wettelijke
verplichting



Overeenkomst



Algemeen belang



Gerechtvaardigd
belang

Het begint aan de tekentafel

Zorgvuldigheid



Functionaris gegevens-
bescherming



Privacy by design



Impact assessment

Technische en organisatorische maatregelen

Verplichtingen



Register met alle
verwerkingen



Gegevens-
beschermingsbeleid



(Digitale)
beveiliging

Mensen moeten controle kunnen uitoefenen

Rechten van de betrokkenen



Recht om
in te zien



Recht om
te wijzigen



Recht om vergeten
te worden



Recht om gegevens
over te dragen



Recht op
informatie

De AVG geldt vanaf 25 mei 2018



Gegevens zijn
beschermd!



U heeft een goed privacyverhaal



Voor uw
doelgroep



Voor de
Autoriteit Persoonsgegevens