Privacy gedragscode Spinoza medewerkers

Datum:	Auteur:	Aanpassingen:
4 april 2018	Tonny Plas	Document aangemaakt en ingevuld
10 september 2018	Daniël Begović	Hoofdstukken aangepast, WhatsApp toegevoegd.
19 september 2018	Daniel Begović	Bijlage toegevoegd, links naar bijlage toegevoegd en lay-out aanpassingen.

Deze gedragscode is bedoeld om medewerkers van Scholengroep Spinoza te attenderen op hun rol met betrekking tot privacybescherming van persoonsgegevens. Iedere medewerker is gehouden deze gedragscode te volgen .

1. Verwerken van persoonsgegevens

1.1. Je legt gegevens in het leerlingdossier zorgvuldig vast en formuleert aantekeningen in het logboek op een professionele wijze.

Persoonsgegevens mogen volgens de wet worden ingezien en opgevraagd worden door ouders/verzorgers van de leerlingen. Zorg ervoor dat je zo feitelijk, zakelijk en objectief mogelijk gegevens vastlegt.

1.2. Je downloadt en bewerkt persoonsgegevens alleen op een device van de school of op een device dat aan de beveiligingseisen van de school voldoet.

De verwerking van persoonsgegevens valt onder de Algemene Verordening Gegevensbescherming (AVG). Als een device kwijt raakt, kan dit als gevolg bijvoorbeeld een datalek hebben. De school kan als gevolg hiervan een boete van de AP (Autoriteit Persoonsgegevens) krijgen. Systemen zoals Magister en de computers van de school zijn daarom extra beveiligd om risico's op een datalek te voorkomen.

1.3. Je slaat leerlinggegevens na bewerking in Magister op. Indien dit niet mogelijk is, worden persoonsgegevens bewaard volgens de AVG normen.

Verlies van (persoons)gegevens moet te allen tijde voorkomen worden. Wees daarom zorgvuldig met waar je de gegevens bewaart, ook als het gaat om gegevens op papier. Het opslaan van persoonsgegevens op een onbeveiligde USB-stick is bijvoorbeeld niet aan te raden.

2. Toegang tot persoonsgegevens

2.1. Je bewaart de device die je van school in bruikleen hebt gekregen altijd op een veilige plek als hij niet gebruikt wordt, zowel thuis als op school.

Het is een ‘open deur’, maar toch wordt het soms wel erg makkelijk gemaakt om devices te ontvreemden. Maak elkaar er dus op attent als je een device onbeheerd ziet liggen.

2.2. Je meldt je computer altijd af als je je werkplek verlaat en je zorgt ervoor dat er op de werkplek geen gevoelige informatie zichtbaar of voor het grijpen ligt.

Met de combinatie van de Windows knop (zie bijlage 1) en L-toets kun je makkelijk jouw device vergrendelen. Maak er een gewoonte van om papieren met gevoelige informatie op een veilige locatie te bewaren of te vernietigen.

2.3. Je laat je internetbrowser geen wachtwoorden van systemen met persoonsgegevens onthouden en je schrijft je logingegevens nooit op. Gebruik in plaats daarvan een wachtwoordkluis.

Zonder dat je er erg in hebt, klik je de optie ‘wachtwoord onthouden’ in je browser aan. Heel makkelijk als je vaak moet inloggen, maar iemand anders die je computer gebruikt kan dan dus ook inloggen als hij of zij op jouw account ingelogd is.

2.4. Je houdt je inloggegevens altijd voor jezelf.

Je login is in feite een sleutel om toegang te krijgen tot de informatie die voor jou toegankelijk moet zijn. Daarnaast herkent het systeem jou door je login, zodat het kan bijhouden wie welke gegevens heeft toegevoegd of gewijzigd.

2.5. Je zet je digibord op “freeze” (zie bijlage 3) voordat je wachtwoorden intoetst of persoonsgegevens in je scherm ziet staan.

Voordat je het weet zien leerlingen gevoelige gegevens of kunnen ze aan de hand van je afgekeken gebruikersnaam en wachtwoord proberen in te loggen.

3. Communiceren of delen van persoonsgegevens

3.1. Je verstuurt nooit bijzondere persoonsgegevens per e-mail. Verwijs bij collega's naar de bewaarplaats van de gegevens en houd je bij externen die om informatie vragen aan de afspraken die door de school met hen zijn gemaakt. Bewaar en deel bijzondere persoonsgegevens nooit via een USB-stick.

In plaats van mailen, kun je een collega aanspreken met de vraag waar de vindplaats van de benodigde gegevens is. Mocht het niet lukken om een collega aan te spreken dan kan er een e-mail worden verstuurd naar de desbetreffende collega. Wel kun je berichten versturen via Magister. Ook kun je gegevens delen via Google drive. Hier geldt het motto "niet mailen maar delen". In bijlage 4 vind je informatie over wat nou bijzondere persoonsgegevens zijn.

3.2. Beeldmateriaal van leerlingen en collega's deel je nooit (bijv. via social media) zonder expliciete toestemming.

Volgens de AVG moeten kinderen onder de 16 jaar schriftelijke toestemming krijgen van hun ouders om op een foto of video te verschijnen. Kinderen van 16 jaar en ouder mogen deze toestemming zelf geven. Mocht er een foto verschijnen waar een leerling die geen toestemming heeft op staat, dan kan de ouder of de leerling zelf een klacht indienen bij de AP. Dit wordt gezien als een datalek.

3.3. Je gebruikt de accounts die door de school worden beheerd als je met ouders of leerlingen wil communiceren via e-mail of social media.

Ouders weten hierdoor dat er met school wordt gecommuniceerd en niet met een privépersoon.

3.4. Je zorgt ervoor dat er bij het voeren van vertrouwelijke (telefonische) gesprekken niet meegeluisterd kan worden.

Vertrouwelijke gesprekken moeten ook vertrouwelijk blijven. Trek je daarom even terug als het telefoongesprek een vertrouwelijk karakter heeft of krijgt.

3.5. Je klikt alleen op linkjes en/of opent alleen bijlagen in e-mails van betrouwbare afzenders.

Virussen kunnen makkelijk worden binnengehaald via (phishing)mails. Dit is een veelgebruikte methode om aan jouw gegevens te komen. Ook kunnen zo de gegevens op je computer versleuteld worden (ransomware).

3.6. Zet de mailadressen in de BCC regel als je naar grotere groepen mensen een mail verstuurt.

Als je dit niet doet, kunnen de ontvangers alle e-mailadressen zien die de ontvanger in de e-mail geplaatst heeft. Zorg er dus voor dat je de e-mailadressen in de BCC zet. Een BCC zorgt er namelijk voor dat degene die het e-mailadres ontvangt niet de e-mailadressen van anderen ziet.

3.7. Je mag geen video, foto's of individuele persoonsgegevens delen via social-mediagroepen.

Tegenwoordig komt het voor dat medewerkers in bijvoorbeeld WhatsApp-groepen komen die door leerlingen aangemaakt zijn. Hierdoor kan een datalek ontstaan. Het opslaan van WhatsApp-gegevens kan ook in Google Drive, wat sterk aan te raden is.

3.8. Je mag niet participeren in social-mediagroepen waaraan leerlingen deelnemen. Uitzonderingen hierop zijn mogelijk voor specifieke situaties, uitsluitend na overleg met de privacy officer van jouw school.

Mocht er iets misgaan in de groep (zoals bijvoorbeeld een WhatsApp groep), dan is de medewerker (en de school) verantwoordelijk. Ook als leerlingen de groep zelf aanmaken, mag een medewerker aan deze groep niet deelnemen.

Er gaat iets fout: wat doe ik dan?

- **Je meldt de volgende en soortgelijke voorvallen direct via** privacy@scholengroepspinoza.nl **vanwege de 'meldplicht datalekken.**
    - Er zijn persoonsgegevens verloren gegaan
    - Je laptop met persoonsgegevens is gestolen
    - Je bent je USB-stick e.d. met persoonsgegevens kwijtgeraakt
    - Je hebt een virus op je device waardoor je niet meer bij je bestanden kunt.
    - Je logingegevens van Magister o.i.d. zijn in handen van anderen gekomen (of je kunt dit niet uitsluiten).
    - Etc.

Mocht er meer informatie gewenst zijn dan kunnen jullie een e-mail sturen naar privacy@scholengroepspinoza.nl of de Privacy Officer op de school waar je werkt.

Bijlage 1: Locken van jouw computer

Bron: SoS-pc

De Windows knop bevindt zich linksonder op het toetsenbord, links van de Alt knop en rechts van de Ctrl (Control) knop.

Bijlage 2: Eisen mobiele devices

Eisen mobiele devices

De mobiele devices in eigendom van de medewerker kunnen gebruikt worden voor schoolwerkzaamheden indien ze voorzien zijn van de volgende beveiligingen, zodat persoonsgegevens goed beschermd zijn:

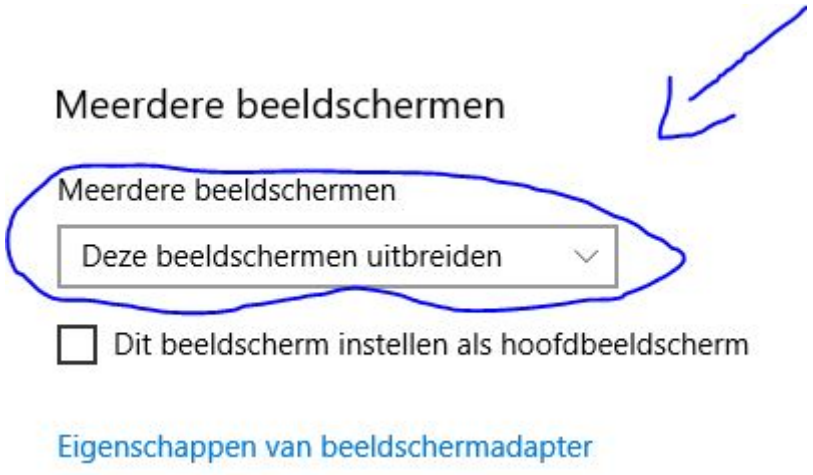
- Het device is voorzien van een wachtwoord of code
- Het device is voorzien van antivirussoftware
- E-mail en andere apps of online toepassingen van de school moeten afgeschermd worden met een apart wachtwoord
- E-mail en andere apps of online toepassingen mogen niet toegankelijk zijn voor andere gebruikers
- Wachtwoorden mogen niet onthouden worden in de browser
- Er worden geen bestanden lokaal opgeslagen, maar alleen op de daarvoor aangewezen bewaarplaatsen van de school
- Er worden geen leerlinggegevens op devices verwerkt die gebruikt worden in openbare netwerken

Bijlage 3: Freezen van het beeldscherm

Hoe ‘’freeze’’ jij je beeldscherm nou? Dit doe je als volgt:

Stap 1. Op je bureaublad: druk op de rechtermuisknop. Vervolgens zie je ‘beeldscherminstellingen’ onderaan het venster. Klik hierop.

Stap 2: Als je in het menu dat verschijnt zit, scroll je naar beneden, totdat je een venster ziet dat ‘Meerdere beeldschermen’ heet. Druk op het bijbehorende venster en dan moet je dit zien.



Het uitbreiden van je beeldscherm zorgt er voor dat je computer alle twee de beeldschermen ziet als aparte beeldschermen. Dit zorgt er dus voor dat je bijvoorbeeld Magister op het ene scherm kan hebben en een presentatie op het andere scherm. Op deze manier ‘freeze’ jij je scherm effectief.

Bijlage 4: Wat zijn bijzondere persoonsgegevens?

Bijzondere persoonsgegevens zijn gegevens over iemands:

- ras of etnische afkomst;
- politieke opvattingen;
- godsdienst of levensovertuiging;
- lidmaatschap van een vakbond;
- genetische of biometrische gegevens met oog op unieke identificatie;
- gezondheid;
- seksuele leven;
- strafrechtelijk verleden.

Bron: Autoriteit Persoonsgegevens