

Gedragcode

05-2018

t.b.v. de AVG wetgeving

Voor:

Bestuursleden, docenten, vrijwilligers en deelnemers van Stichting Nationaal Projectmatig
Accordeon Onderwijs

Privacy voorop!

Opgesteld door Annemarieke van der Ploeg
25-05-2018 Markelo

Inhoud:

	Blz.
Hoofdstuk 1: Hiërarchie	3
Hoofdstuk 2: Bevoegdheden	4
Hoofdstuk 3: Doen en laten	6
Bijlage 1: praktische tips AVG	7

Hoofdstuk 1: Hiërarchie

De stichting kent voor privacy voorwaarden de volgende Hiërarchie:

- 1: Bestuur
- 2: Docenten
- 3: Vrijwilligers
- 4: Deelnemers
- 5: Openbaar

Waarbij 1 de meeste bevoegdheden heeft en 5 de minste.

Om persoonlijke informatie te delen met een andere bevoegdheid, controleer je ten alle tijden de gedragscode of dit toegestaan is. Doe je dat niet of negeer je het voorgeschreven protocol, dan riskeer je ontslag en of ben je hoofdelijk aansprakelijk voor mogelijke gevolgen.

Hoofdstuk 2: Bevoegdheden

Hieronder is schematisch weergegeven wie er toegang heeft tot welke gegevens. Als bestuurslid, docent, vrijwilliger of deelnemer volg je dit schema ten alle tijden als het gaat om persoonlijke informatie. Doe je dat niet, dan riskeer je ontslag en/of hoofdelijke aansprakelijkheid.

	Bestuur	Docenten	Vrijwilligers	Deelnemers	Openbaar
<i>Naam</i>	Ja	Ja	Ja	Ja	Nee
<i>Adresgegevens</i>	Ja	Ja	Indien nodig	Nee	Nee
<i>Mail</i>	Ja	Ja	Indien nodig	Nee	Nee
<i>Telefoon</i>	Ja	Ja	Indien nodig	Nee	Nee
<i>Medische gegevens</i>	Ja	Indien nodig	Indien nodig	Nee	Nee
<i>Dieet informatie</i>	Ja	Indien nodig	Indien nodig	Nee	Nee
<i>NAW minderjarigen</i>	Ja	Ja	Indien nodig	Nee	Nee
<i>Geboortedatum deelnemer</i>	Ja	Ja	Nee	Nee	Nee
<i>Audio en visueel materiaal</i>	Ja	Ja	Ja*	Ja*	Ja*
<i>Volledig inzicht inschrijfformulier</i>	Ja	Ja	Nee	Nee	Nee
<i>Bankrekening gegevens</i>	Ja	Nee	Nee	Nee	Nee
<i>Gegevens contactpersoon</i>	Ja	Indien nodig	Indien nodig	Nee	Nee
<i>Deelname gerichte informatie (zoals instrument, docent enz.)</i>	Ja	Ja	Indien nodig	Nee	Nee

Z.o.z.

Specifieke informatie van docenten en bestuursleden:

	Bestuur	Docenten	Vrijwilligers	Deelnemers	Openbaar
<i>VOG</i>	Ja	Nee	Nee	Nee	Nee
<i>IBAN</i>	Ja	Nee	Nee	Nee	Nee
<i>Overeenkomst</i>	Ja	Nee	Nee	Nee	Nee
<i>Visueel materiaal van eigen website</i>	Ja	Ja	Ja	Ja	Ja
<i>Visueel materiaal verzameld tijdens activiteit</i>	Ja	alleen met toestemming	alleen met toestemming	alleen met toestemming	alleen met toestemming
<i>Audio en of video materiaal</i>	Ja	alleen met toestemming	alleen met toestemming	alleen met toestemming	alleen met toestemming

* Tenzij schriftelijk of per mail bezwaar ingediend

Hoofdstuk 3: Doen en laten

Wanneer je als bestuurslid, docent, vrijwilliger **of deelnemer** informatie in handen krijgt, dan is het belangrijk om te weten wat je daar wel en niet mee mag doen. Daarnaast wil je natuurlijk weten hoe je dat het beste kunt aanpakken. Hieronder een opsomming van standaard zaken die je behoort toe te passen wanneer je met persoonsgegevens en/of foto's van anderen te maken krijgt.

- Om je bewust te worden bekijk je de video van Stichting AVG:
<https://youtu.be/QX3JpbPO2Pg>
- Als je persoonlijke gegevens of foto's op je computer bewaard, dan vergrendel je deze met een wachtwoord.
- Fotomateriaal en andere persoonlijke informatie mag je nooit op eigen initiatief delen, vraag eerst toestemming van het bestuur of de persoon zelf (liefst schriftelijk om twijfel bij onenigheid te voorkomen).
- Noem geen namen en andere persoonlijke gegevens als je met mensen buiten de activiteit in gesprek bent.
- Zorg dat je op de hoogte bent van hoofdstuk 2 en controleer het zo nodig. Deel nooit zonder toestemming van het bestuur informatie met een doelgroep die daar in hoofdstuk 2 geen toestemming voor heeft.
- Neem bijlage 1 door en houd je hier aan indien van toepassing.



Praktische tips

- Blokkeer altijd je beeldscherm bij het verlaten van je werkplek;
- Laat documenten met persoonsgegevens nooit onbeheerd achter op bureau of bij de printer;
- Kies nooit voor automatisch opslaan van inloggegevens op je computer;
- Besef dat openbare netwerken niet veilig zijn;
- Let op wat je deelt via sociale media;
- Bedek altijd je webcam om 'meekijken' te voorkomen;
- Gebruik nooit de inlog van een collega en geef je inloggegevens ook niet door aan een collega;
- Zorg ervoor dat je mobiele telefoon beveiligd is met een inlogcode of vingerherkenning.