

AUTEURS

Richard de Koning (Informatieveiligheid en Privacy)
Cebeli Gonul (Juridische Zaken)

STATUS

Finaal Concept – ter vaststelling CvB

VERSIENUMMER

1.9

DATUM

22-6-2020

Reglement Verantwoord Netwerkgebruik

Acceptable use policy

Reglement voor het veilig gebruik
van ICT-voorzieningen voor medewerkers

Model IBPDO26 – Verantwoord Netwerkgebruik

INHOUD

Reglement Verantwoord Netwerkgebruik voor medewerkers	3
Basis voor het reglement	3
Artikel 1. Uitgangspunten	3
Artikel 2. Intellectueel eigendom en vertrouwelijke informatie	4
Artikel 3. Gebruik van computer- en netwerkfaciliteiten	4
Artikel 4. Gebruik van e-mail en andere ICT-communicatiemiddelen	5
Artikel 5 Gebruik van internet	5
Artikel 7. Monitoring en controle	6
Artikel 8. Procedure bij gericht onderzoek	6
Artikel 9. Rechten van de medewerker m.b.t. persoonsgegevens	7
Artikel 10. Consequenties van overtreding	7
Artikel 11. Slotbepaling	7

Reglement Verantwoord Netwerkgebruik voor medewerkers

Basis voor het reglement

Het gebruik van internet en ICT-middelen¹ is voor (veel van) de medewerkers binnen de Instelling noodzakelijk om hun werk goed te kunnen doen. Aan het gebruik hiervan zijn risico's verbonden die het stellen van gedragsregels noodzakelijk maken. Tegen de achtergrond van deze risico's mag van de medewerkers verantwoord gebruik van internet en ICT worden verwacht.

Met dit Reglement wil Stichting Zadkine, hierna te noemen de "Instelling" regels stellen omtrent het gewenst gebruik van deze bedrijfsmiddelen. Het streven daarbij is een goede balans aan te brengen tussen gebruikersgemak en verantwoord en veilig ICT- en internetgebruik.

Afspraken in het kader van privacy worden in een apart reglement geregeld, het "**Privacy reglement voor medewerkers**"

Het gebruik van social media zoals Facebook, LinkedIn en Twitter wordt steeds belangrijker maar kan ook zijn weerslag hebben op de Instelling. Daarom wil de Instelling ook hier bepaalde regels aan stellen. Afspraken omtrent het gebruik van social media zoals Facebook, LinkedIn en Twitter zijn opgenomen in het "**Reglement social media voor medewerkers en studenten**"

Artikel 1. Uitgangspunten

- 1.1. Het Reglement stelt regels ten aanzien van het gebruik van de bedrijfsmiddelen ICT en internet door medewerkers. Doel van deze regels is de goede orde te bepalen ten aanzien van:
 - systeem- en netwerkbeveiliging, inclusief beveiliging tegen schade en misbruik;
 - tegengaan van seksuele intimidatie, discriminatie en andere strafbare feiten;
 - bescherming van privacy gevoelige informatie waaronder en persoonsgegevens van de Instelling en haar medewerkers, en van studenten en ouders;
 - bescherming van vertrouwelijke informatie van de Instelling en haar medewerkers, en van deelnemers en ouders;
 - bescherming van de intellectuele eigendomsrechten van de Instelling en derden waaronder het respecteren van de licentie-afspraken die van toepassing zijn binnen de Instelling;
 - voorkomen van negatieve publiciteit;
 - kosten- en capaciteitsbeheersing.
- 1.2. Beperkt privégebruik van internet en ICT-middelen is alleen toegestaan voor zover het werk er niet onder lijdt. (zie Artikel 4: Gebruik van e-mail en andere ICT-communicatiemiddelen)
- 1.3. Dit Reglement geldt voor een ieder die voor de Instelling werkzaam is, dus ook voor uitzendkrachten en tijdelijke medewerkers. Het Reglement geldt niet voor (gast)deelnemers; hiervoor is het aparte Deelnemersreglement opgesteld.
- 1.4. De Instelling streeft in het kader van handhaving van dit Reglement naar maatregelen die inzage in privacygevoelige informatie of persoonsgegevens van individuele medewerkers zo veel mogelijk beperken. Zij zal waar mogelijk slechts geautomatiseerd controleren of filteren zonder daarbij zichzelf of andere personen inzage te geven in gedrag van individuele personen.

¹ Onder ICT-middelen wordt onder meer verstaan: PC's (computers), laptops, tablets, smartphones, usb-sticks, randapparatuur, smartboards, netwerk en netwerkcomponenten.

Artikel 2. Intellectueel eigendom en vertrouwelijke informatie

- 2.1. De medewerker dient vertrouwelijke informatie en/of persoonsgegevens waar hij in het kader van het werk toegang tot heeft, strikt vertrouwelijk te behandelen en voldoende maatregelen te treffen om de vertrouwelijkheid te waarborgen.
Hieronder valt ook de 'clean desk en clean screen policy': dit betekent dat er geen belangrijke informatie zichtbaar is of bereikbaar is voor mensen die deze informatie niet mogen zien.
De medewerker vergrendelt het scherm van de computer als deze kortere of langer tijd de werkplek verlaat. Bij vertrek sluit de medewerker de computer af en maakt de werkplek vrij van vertrouwelijke informatie.
- 2.2. De medewerker maakt geen inbreuk op de intellectuele eigendomsrechten van de Instelling en derden en respecteert licentieafspraken zoals die van toepassing zijn binnen de Instelling.
- 2.3. De zeggenschap over de informatie van de Instelling berust bij Instelling. De medewerker heeft geen zelfstandige zeggenschap over de informatie behalve als hem dat expliciet is toegekend door de Instelling.
- 2.4. De medewerker besteedt bijzondere aandacht aan het treffen van maatregelen zoals in dit Reglement genoemd, indien in het kader van het uitvoeren van de werkzaamheden de verwerking van vertrouwelijke informatie buiten de Instelling noodzakelijk is zoals via E-mail, in niet instellingsgebonden Cloud-toepassingen, op externe opslagmedia of eigen client-apparatuur (USB-apparaten, Tablets, etc.).
Indien de Instelling met betrekking tot het waarborgen van de vertrouwelijkheid voorschriften heeft opgesteld zal medewerker deze strikt naleven.
Medewerkers zijn verplicht vermoedens van misbruik, lekken van vertrouwelijke informatie of zwakke plekken op het gebied van informatieveiligheid en privacy (IVP) te melden via het IVP-portaal of Servicedesk.

Artikel 3. Gebruik van computer- en netwerkfaciliteiten

- 3.1. Computer- en netwerkfaciliteiten worden beschikbaar gesteld aan de medewerker voor gebruik in het kader van zijn functie. Gebruik is derhalve verbonden aan taken die voortvloeien uit deze functie. Privégebruik van deze middelen is alleen toegestaan zoals bepaald in artikel 1.2.
- 3.2. De medewerker dient te allen tijde zorgvuldig om te gaan met aan hem persoonlijk toegekende inloggegevens en eventuele aanvullende authenticatiemiddelen (zoals smartcards en tokens). Persoonsgebonden wachtwoorden en aanvullende authenticatiemiddelen mogen niet worden gedeeld. Bij een vermoeden van misbruik van een wachtwoord kan de ict-beheerder per direct het betrokken account ontoegankelijk maken.
- 3.3. Het aansluiten van servers en actieve netwerkcomponenten (zoals access points en routers is niet toegestaan zonder toestemming van de ict-beheerder.

De ict-beheerder kan aan de toestemming regels verbinden ter handhaving van dit reglement, zoals het moeten installeren van virusscanners en wachtwoord-beveiliging.

Het aansluiten van eigen client-apparatuur (zoals laptops, tablets en telefoons) is alleen toegestaan op de daarvoor beschikbaar gestelde (wireless) netwerkaansluitingen. De ict-beheerder kan aan de toegang tot deze aansluitingen regels verbinden ter handhaving van dit reglement, zoals het moeten installeren van virusscanners en wachtwoordbeveiliging.
- 3.4. Het opslaan van privébestanden of -informatie op systemen van de Instelling is toegestaan, mits dit niet leidt tot overbelasting van de opslagcapaciteit van deze systemen of een verstoring van de goede orde op de werkvloer. De Instelling is echter niet verplicht van dergelijke bestanden of informatie reservekopieën te maken of kopieën beschikbaar te stellen bij vervanging of reparatie van de betreffende systemen.
- 3.5. Het gebruik van computer- en netwerkfaciliteiten door de medewerker ten behoeve van nevenwerkzaamheden is uitsluitend toegestaan als en voor zover de Instelling hiervoor schriftelijk toestemming heeft verleend.

Artikel 4. Gebruik van e-mail en andere ICT-communicatiemiddelen

- 4.1. Het e-mailsysteem en de bijbehorende mailbox en het e-mailadres wordt aan de medewerker voor gebruik in het kader van zijn functie beschikbaar gesteld. Gebruik is derhalve verbonden aan taken die voortvloeien uit deze functie.
- 4.2. Privégebruik van deze middelen is alleen toegestaan zoals bepaald in artikel 1.2.
- 4.3. Verboden bij elk gebruik (privé of niet) van ICT-communicatiemiddelen is echter:
 - het verzenden van berichten met een pornografische, racistische, discriminerende, bedreigende, beledigende of aanstootgevende inhoud;
 - het verzenden van berichten met een (seksueel) intimiderende inhoud;
 - het verzenden van berichten die (kunnen) aanzetten tot discriminatie, haat en/of geweld;
 - het versturen van ongevraagde berichten aan grote aantallen ontvangers, kettingbrieven of kwaadaardige software zoals virussen, Trojaanse paarden of spyware.
- 4.4. De medewerker gebruikt voor privémail bij voorkeur niet het door de Instelling verstrekte e-mail adres, binnen de grenzen van artikel 1.2. De organisatie zal de toegang tot andere e-maildiensten niet blokkeren of specifiek monitoren.
- 4.5. In geval van ziekte, onverwacht langdurige afwezigheid of disfunctioneren van de medewerker, doch uitsluitend als dit een zwaarwegende reden van bedrijfsbelang tot toegang oplevert, is de Instelling gerechtigd een vervanger of leidinggevende toegang tot de bestanden of mailbox van de medewerker te verschaffen doch uitsluitend nadat hiertoe expliciet toestemming van de directeur van de medewerker is verkregen en dit door de directeur kenbaar is gemaakt aan de betreffende medewerker. Deze mag zich echter geen toegang verschaffen tot als privé gemarkeerde mappen, als privé herkenbare mails, of mails verzonden naar dan wel afkomstig van een vertrouwenspersoon of bedrijfsarts. Indien de medewerker geen dergelijke markeringen heeft aangebracht, kan de Instelling door inschakeling van een vertrouwenspersoon de betreffende informatie van de medewerker controleren om zo privéinformatie te herkennen en te separeren alvorens de vervanger of leidinggevende toegang krijgt.

Dit Artikel 4.5 is ter goedkeuring voorgelegd aan de OR (WOR, artikel 27, lid K).
- 4.6. E-mailberichten van leden van het medezeggenschapsorgaan onderling, van bedrijfsartsen en van een ieder die zich op grond van de wet op vertrouwelijkheid mag beroepen, worden niet gecontroleerd. Dit geldt niet voor geautomatiseerde controle op de veiligheid van het e-mailverkeer en netwerk.

Artikel 5 Gebruik van internet

- 5.1. De toegang tot internet en bijbehorende faciliteiten worden aan de medewerker voor gebruik in het kader van zijn functie beschikbaar gesteld. Gebruik is derhalve verbonden aan taken die voortvloeien uit deze functie.
- 5.2. Privégebruik van deze middelen is alleen toegestaan zoals bepaald in artikel 1.2.
- 5.3. Verboden bij elk gebruik (privé of niet) is echter:
 - sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten;
 - filesharing-, media- of streamingdiensten (zoals Spotify of Netflix) te gebruiken wanneer dit overmatig veel dataverkeer genereert, zodanig dat het de beschikbaarheid van de faciliteiten in gevaar kan brengen;
 - films, muziek, software en overig auteursrechtelijk beschermd materiaal te downloaden van enige illegale bron of wanneer de medewerker daadwerkelijk weet dat dit in strijd met auteursrechten is;
 - films, muziek, software en overig auteursrechtelijk beschermd materiaal te verspreiden (uploaden) naar derden zonder toestemming van de rechthebbenden.

- 5.4. Het gebruik van social media zoals Facebook, Twitter, YouTube etcetera is gebonden aan de bepalingen die zijn opgenomen in het “**Reglement social media voor medewerkers en studenten**”

Artikel 7. Monitoring en controle

- 7.1. Controle van gebruik van de ICT-faciliteiten en internetgebruik vindt slechts plaats in het kader van handhaving van de regels uit dit reglement voor de doelen genoemd in Artikel 1.
- 7.2. Ten behoeve van controle op de naleving van de regels worden gegevens geautomatiseerd verzameld (gelogd). Deze gegevens zijn alleen toegankelijk voor de direct verantwoordelijke systeembeheerders en worden alleen in geanonimiseerde vorm aan overige beheerders en andere verantwoordelijken beschikbaar gesteld. Deze kunnen tot nadere technische maatregelen besluiten.
- 7.3. Bij vermoedens van overtreding van de regels kan controle worden uitgevoerd op het niveau van individuele verkeersgegevens van het e-mail- en internetgebruik. Slechts bij zwaarwegende redenen vindt controle op de inhoud plaats.
- 7.4. De Instelling houdt zich bij het controleren op het niveau van verkeersgegevens of persoonsgegevens onverkort aan de AVG en andere relevante wet- en regelgeving. In het bijzonder beveiligd de Instelling de bij controle vastgelegde gegevens tegen ongeautoriseerde toegang en zijn personen met toegang daartoe contractueel verplicht tot geheimhouding.
- 7.5. Enkele specifieke maatregelen ter controle die de Instelling kan voeren, zijn:
- controle ter voorkoming van negatieve publiciteit en seksuele intimidatie en de controle in het kader van systeem- en netwerkbeveiliging vindt plaats op basis van filtering van de inhoud op trefwoorden en categorisering van (web)inhoud. Verdachte berichten worden automatisch teruggestuurd naar de afzender;
 - controle van netwerkbelasting en het blokkeren of beperken van de netwerkcapaciteit voor niet-essentiële netwerkdiensten wordt beperkt tot het op basis van verkeersgegevens nagaan van de bronnen van kosten of capaciteitsvraag (zoals de adressen van internetradio en videosites). Als deze websites tot grote kosten of overlast leiden, worden zij geblokkeerd of afgeknepen, zonder daarbij de vertrouwelijkheid van de inhoud van de communicatie te schenden;
 - controle op het gebruik van beeldmateriaal vindt plaats op basis van klachten of meldingen van derden, of steekproefsgewijs bij beeldmateriaal dat openbaar beschikbaar is.

Artikel 8. Procedure bij gericht onderzoek

- 8.1. Van gericht onderzoek is sprake wanneer verkeersgegevens of andere persoonsgegevens betreffende een specifieke medewerker worden vastgelegd in het kader van een onderzoek naar aanleiding van een zwaarwegend vermoeden van een overtreding van dit Reglement door die medewerker.
- 8.2. Gericht onderzoek vindt uitsluitend plaats na schriftelijke opdracht van de directeur van de betreffende school. Het College van Bestuur ontvangt een afschrift van deze opdracht en een vastlegging van de resultaten van het onderzoek. Indien het onderzoek geen aanleiding geeft tot verdere maatregelen wordt de vastlegging vernietigd.
- 8.3. In afwijking van het vorige lid vindt gericht onderzoek naar de beveiliging of integriteit van randapparatuur plaats door de ict-beheerder op basis van concrete aanwijzingen. Aparte toestemming van de in lid 2 bedoelde instantie is niet nodig. De resultaten van dit onderzoek worden alleen gedeeld met de medewerker met het doel de beveiliging of integriteit van de randapparatuur te verbeteren. Bij herhaling zal de procedure uit lid 2 worden gevolgd.
- 8.4. Gericht onderzoek beperkt zich in eerste instantie tot verkeersgegevens van het gebruik van de faciliteiten. Als gericht onderzoek nader bewijs oplevert, kan de Instelling overgaan tot het kennismaken van de inhoud van communicatie of opgeslagen bestanden. Dit vereist schriftelijke toestemming van het College van Bestuur, welke toestemming de redenen zal noemen waarom deze

wordt verleend. De Instelling zal zich maximaal inspannen de identiteit van de personen die deze kennisneming uitvoeren, geheim te houden. De vastlegging wordt onder naam van de directeur gedaan.

- 8.5. Enkele specifieke persoonsgebonden maatregelen ter controle die de Instelling kan voeren, zijn:
- controle op het uitlekken van vertrouwelijke informatie vindt plaats op basis van steekproefsgewijze controle op trefwoorden. Verdachte berichten worden apart gezet voor nader onderzoek in overleg met het bestuur;
 - controle op overtreding van het verbod uit Artikel 4 lid 3 vindt plaats door twee personen op klacht [of steekproefsgewijs] e-mailberichten te openen en de inhoud te raadplegen. Deze personen zijn gebonden aan geheimhouding over de inhoud;
- 8.6. De medewerker wordt zo spoedig mogelijk schriftelijk geïnformeerd door de directeur over de aanleiding, de uitvoering en het resultaat van het onderzoek. De medewerker wordt in de gelegenheid gesteld uitleg te geven over de aangetroffen gegevens. Uitstel van het informeren mag alleen als informeren het onderzoek daadwerkelijk zou kunnen schaden.
- 8.7. Systeembeheerders verschaffen zich slechts toegang tot accounts of computers van medewerkers als de medewerker daarvoor zijn toestemming heeft gegeven. Toegang zonder deze toestemming is slechts toegestaan in dringende gevallen of bij een duidelijk vermoeden van schending van dit Reglement, zoals nader bepaald in dit Artikel. De medewerker zal in dat geval achteraf worden geïnformeerd.

Artikel 9. Rechten van de medewerker m.b.t. persoonsgegevens

Zie: **“Privacy reglement voor medewerkers”**

Artikel 10. Consequenties van overtreding

- 10.1. Bij handelen in strijd met dit Reglement of de algemeen geldende wettelijke regels, kan het bestuur afhankelijk van de aard en de ernst van de overtreding disciplinaire maatregelen treffen. Hieronder vallen een waarschuwing, berisping, overplaatsing, schorsing en beëindiging van de arbeidsovereenkomst. Daarnaast kan het bestuur besluiten tot een al dan niet tijdelijke beperking in de toegang tot bepaalde ICT-faciliteiten.
- 10.2. Disciplinaire maatregelen (behalve een waarschuwing) kunnen niet worden getroffen enkel op basis van een langs geautomatiseerde uitgevoerde verwerking van persoonsgegevens, zoals een constatering van een automatisch filter of blokkade. Voorts worden geen disciplinaire maatregelen getroffen zonder dat de medewerker gelegenheid heeft gekregen zijn zienswijze naar voren te brengen.
- 10.3. Aanvullend op voorgaande is het mogelijk dat de Instelling bij (geautomatiseerde) constatering van overlast een tijdelijke blokkade van de betreffende faciliteit invoert. Deze blokkade zal zolang worden gehandhaafd tot aangetoond is dat de oorzaak is weggenomen. Bij herhaling van de oorzaak kunnen disciplinaire maatregelen worden genomen.

Artikel 11. Slotbepaling

- 11.1. Dit Reglement wordt jaarlijks geëvalueerd door het College van Bestuur van Stichting Zadkine. De Instelling betreft medezeggenschapsorganen bij de evaluatie/Medezeggenschapsorganen kunnen ook zelfstandig het advies nemen het Reglement te evalueren. De eerstkomende evaluatie vindt plaats in januari 2021
- 11.2. Stichting Zadkine kan dit Reglement met instemming van het medezeggenschapsorgaan wijzigen als de omstandigheden daar aanleiding toe geven. Voorgenomen wijzigingen worden voorafgaand aan de invoering aan de medewerkers bekend gemaakt. Het College van Bestuur zal feedback van medewerkers in overweging nemen alvorens de wijzigingen in te voeren.
- 11.3. In gevallen waarin dit Reglement niet voorziet, beslist het College van Bestuur.

