ZADKINE

IM-IT

Gedragscode medewerkers voor computer- en internetgebruik

Acceptable use policy, voor het veilig gebruik van ICT-voorzieningen;

Auteur(s): Samenwerking tussen SURFibo en SURFnet
Bewerkt door: Richard de Koning en Jack Haagen
Revisie: Cebeli Gonul (Juridische Zaken)

Versie: 1.0
Datum: 29-1-2018

REGIEGROEP IBP IN HET MBO
Kennisnet SURF saMBO-ICT

Dit ICT-reglement van Zadkine is gebaseerd op IBPDOC26 – Verantwoord netwerk gebruik, Versie 2.0, september 2017

Versiebeheer

Versie	Datum	Auteur	Aard wijzigingen / review	Status
0.1	12-10-2017	Richard de Koning	Eerste opzet	Concept
0.2	16-10-2017	Richard de Koning	Basisdocument IPBDOC26 gecombineerd met Good Practices saMBO-ICT en aangepast aan Zadkine	Concept
0.3	17-10-2017	Richard de Koning	Ter controle aanbieden aan FG voor verdere reviews	Concept
0.4	29-1-2018	Richard de Koning en Jack Haagen	Aanpassingen n.a.v. revisies Juridische Zaken en logo vervangen	Concept
1.0	4-4-2018	Richard de Koning en Jack Haagen	Akkoord door de Regiegroep Informatievoorziening	Definitief

ZADKINE

Inhoudsopgave

Reglement verantwoord netwerkgebruik

Basis voor het reglement

Het gebruik van internet en ICT-middelen 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 de instelling, 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 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.

Zie concept bijlage: Protocol social media voor medewerkers en studenten

De Instelling is als werkgever bevoegd regels te stellen omtrent de uitvoering van het werk en de goede orde op de werkvloer, zo volgt uit de wet.

Artikel 1. Uitgangspunten

1.1 Doel van het reglement

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 persoonsgege-vens van de Instelling en haar medewerkers, en van studenten en ouders;
- bescherming van vertrouwelijke informatie van de Instelling en haar mede-werkers, en van studenten 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. Privégebruik Internet en ICT-middelen

Beperkt privégebruik van internet en ICT-middelen is alleen toegestaan tijdens pauzes en/of voor zover het werk er niet onder lijdt.

1.3. Geldigheid

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)studenten; hiervoor is het aparte Studentenreglement opgesteld.

1.4. Controle

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.

Artikel 2. Intellectueel eigendom en vertrouwelijke informatie

2.1. Vertrouwelijke informatie

De medewerker dient vertrouwelijke informatie, privacygevoelige informatie waaronder 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.

2.2. Intellectueel eigendom

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. Informatie van de instelling

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. Externe verwerking vertrouwelijke informatie

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.

2.5. Systeembeheerders

Deze bepalingen gelden in het bijzonder voor systeembeheerders, voor wie schending van deze bepalingen als plichtsverzuim wordt aangemerkt, gezien hun bijzondere positie.

Artikel 3. Gebruik van computer- en netwerkfaciliteiten

3.1. Beschikbaarheid faciliteiten

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. Inloggegevens

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, wachtzinnen 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. Voorgeschreven systemen

De Instelling kan voor onderwijs- en andere bedrijfsdoeleinden systemen of applicaties voorschrijven, zoals een Elektronische Leeromgeving, een emailsysteem,(Mobiele) Applicaties (Apps), Cloudvoorzieningen of multimediadiensten.

De werknemer zal voor het delen van lesmateriaal of het uitvoeren van onderzoek alleen deze systemen gebruiken en de daarbij gestelde beperkingen en eisen stipt naleven.

3.4. Installeren van software en aansluiten apparatuur

Het installeren van software op de computer- en netwerkfaciliteiten van de organisatie is niet toegestaan zonder aparte toestemming van de ict-beheerder. Ook 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.

3.5 Opslaan van privébestanden

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. Nevenwerkzaamheden

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. E-mail

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 middelen

Privégebruik van deze middelen is alleen toegestaan zoals bepaald in artikel 1.2.

4.3. Verboden gebruik e-mail

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 te versturen of kwaadaardige software zoals virussen, Trojaanse paarden of spyware te versturen.

4.4. Privégebruik e-mail

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. Toegang door instelling

In geval van ziekte, onverwacht langdurige afwezigheid of grove nalatigheid 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 Functionaris Gegevensbescherming van de instelling en 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, aangewezen door de Functionaris Gegevensbescherming, de betreffende informatie van de medewerker controleren om zo privéinformatie te herkennen en te separeren alvorens de vervanger of leidinggevende toegang krijgt.

4.6. Controle vertrouwelijkheid

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. Toegang tot Internet

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 Internet

Privégebruik van deze middelen is alleen toegestaan zoals bepaald in artikel 1.2.

5.3. Verboden gebruik Internet

Verboden bij elk gebruik (privé of niet) is echter:

- sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten;
- filesharing- of streamingdiensten (zoals internetradio of Uitzendinggemist) 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.

Artikel 6. Gebruik van sociale media

6.1. Gebruik

De Instelling ondersteunt de open dialoog en de uitwisseling van ideeën en het delen van kennis van de medewerker met vakgenoten en derden via sociale media (zoals Facebook, Youtube, MSN, Skype, Omegle, Twitter of Linkedin), voor zover dit om professionele uitingen gaat die bijdragen aan het werk van betrokken medewerker. Indien dit werkgerelateerde onderwerpen betreft, dient de medewerker altijd de Instelling en zijn functie te vermelden, alsmede een disclaimer waarin staat dat het een persoonlijk standpunt betreft, dat niet overeen hoeft te komen met dat van de Instelling.

6.2. Contact met studenten op social media

Medewerker zal geen studenten toevoegen als ‘vrienden’ of contacten op dergelijke sociale media, tenzij hij hiertoe een apart profiel hanteert dat duidelijk aan de Instelling gelinkt is en waar de Instelling eisen ten aanzien van presentatie, inhoud en functioneren aan kan stellen.

6.3. Bijzondere verantwoordelijkheid

Bestuurders, managers, leidinggevenden en anderen die namens de Instelling beleid of strategie uitdragen hebben een bijzondere verantwoordelijkheid bij het gebruik van sociale media, ook als de inhoud niet direct verband houdt met hun werk. Op grond van hun positie moeten zij nagaan of zij op persoonlijke titel kunnen publiceren. Zij zijn zich ervan bewust dat medewerkers lezen wat zij schrijven.

6.4. Deelname vanaf privédomein

Dit artikel geldt ook indien medewerkers vanaf privécomputers of -internetaansluitingen deelnemen aan sociale media, doch uitsluitend voor zover het gaat om deelname die het werk kan raken.

6.5. Werkgerelateerd social media account verbonden aan persoon

Wanneer medewerker een sociale-media-account opzet dat direct werkgerelateerd is, terwijl het op naam van medewerker persoonlijk is gesteld, zullen medewerker en de Instelling bij beëindiging van het dienstverband een passende oplossing zoeken voor het overdragen van dit profiel of de informatie en contacten daarop.

Artikel 7. Monitoring en controle

7.1. Controle gebruik

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. Verboden gebruik van de bedrijfsmiddelen wordt zo veel mogelijk langs technische weg onmogelijk gemaakt.

7.2. Logging van gegevens

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. Vermoedens van overtreding

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. Wet Bescherming Persoonsgegevens

De Instelling houdt zich bij het controleren op het niveau van verkeersgegevens of persoonsgegevens onverkort aan de Wet bescherming persoonsgegevens en andere relevante wet- en regelgeving. In het bijzonder beveiligt de Instelling de bij controle vastgelegde gegevens tegen ongeautoriseerde toegang en zijn personen met toegang daartoe contractueel verplicht tot geheimhouding.

7.5. Specifieke maatregelen

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. Verdachte berichten worden automatisch teruggestuurd naar de afzender;
- controle in het kader van kosten- en capaciteitsbeheersing 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. Definitie

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. Opdrachtgever

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. Randapparatuur

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. Reikwijdte

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 kennisnemen 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. Specifieke maatregelen ter controle

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. Kennisgeving

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. Toegang door systeembeheerders

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

Is beschreven in het Privacy reglement voor medewerkers

Artikel 10. Consequenties van overtreding

10.1. Disciplinaire maatregelen

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. Uitzonderingen

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.

10.3. Blokkade

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. Evaluatie Reglement

Dit Reglement wordt jaarlijks geëvalueerd door het College van Bestuur van de Instelling. De Instelling betrekt medezeggenschapsorganen bij de evaluatie/Medezeggenschapsorganen kunnen ook zelfstandig het advies nemen het Reglement te evalueren. De eerstkomende evaluatie vindt plaats in [MAAND JAAR].

11.2. Wijzigen Reglement

De Instelling 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. College van Bestuur

In gevallen waarin dit Reglement niet voorziet, beslist het College van Bestuur.