ICT-gedragscode medewerkers van Onderwijsgroep Tilburg

Auteur(s): Samenwerking tussen SURFibo en SURFnet

Bewerkt door: Bram Bogers, Niels Dutij

Vastegsteld: CvB/1718.053

Datum: 23 april 2018

De ICT-reglementen voor medewerkers en deelnemers van Onderwijsgroep Tiburg zijn gebaseerd op Model reglementen voor het Hoger Onderwijs, een gezamenlijk product van SURFnet en SURFibo.

Deze publicatie is gelicenseerd onder een Creative Commons Naamsvermelding 3.0 Unported licentie
Meer informatie over deze licentie vindt u op http://creativecommons.org/licenses/by/3.0/deed.nl

ICT-gedragscode medewerkers van Onderwijsgroep Tilburg

1 Preambule

Het gebruik van internet en ICT-middelen[1] 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.

Het gebruik van sociale media platformen zoals Facebook, LinkedIn en Twitter wordt steeds belangrijker en kan ook zijn weerslag hebben op de Instelling. Daarom wil de Instelling ook hier bepaalde regels aan stellen.

Met dit Reglement wil de Onderwijsgroep Tilburg (hierna te noemen de "Instelling") regels stellen omtrent het gewenst gebruik van deze bedrijfsmiddelen. Het gaat daarbij om een verantwoord en veilig ICT- en internetgebruik.

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

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

Artikel 1. Uitgangspunten

1.1. Het Reglement stelt regels ten aanzien van het gebruik van de ICT-middelen en internet door medewerkers. Het gaat daarbij om:

- systeem- en netwerkbeveiliging, inclusief beveiliging tegen schade en misbruik;
- tegengaan van seksuele intimidatie, discriminatie en andere strafbare feiten;
- bescherming van privacy-gevoelige informatie van de Instelling en persoonsgegevens van de medewerkers, deelnemers en ouders;
- bescherming van vertrouwelijke informatie van de Instelling, de medewerkers, 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 tijdens pauzes en/of voor zover het werk er niet onder lijdt.

1.3. Dit Reglement geldt voor een ieder die voor de Instelling werkzaam is, dus ook voor uitzendkrachten, tijdelijke medewerkers en staigiares.

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.

1.5. De Instelling kan het recht tot gebruik van (een deel van) het internet en de ICT-middelen verlenen, maar ook altijd weer intrekken.

---

[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 en/of 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. De medewerker maakt geen inbreuk op de intellectuele eigendomsrechten van de Instelling en derden en respecteert licentieafspraken 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 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 de medewerker deze strikt naleven.

2.5 Onder de maatregelen zoals bedoeld in artikel 2.4, valt in ieder geval de verplichting voor de mewerker om gebruik te maken van versleutelde externe opslagmedia of versleutelde eigen client-apparatuur.

2.6 De medewerker is verplicht om zijn computer te vergrendelen als hij zijn werkplaats verlaat.

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.

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

3.3. 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 account is de ICT-beheerder geautoriseerd per direct het betrokken account ontoegankelijk te maken en de rechten op het gebruik van het netwerk van de medewerker in te trekken.

3.4. Het installeren van software op de computer- en netwerkfaciliteiten van de organisatie is niet toegestaan zonder expliciete 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 mobiele 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. 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.

3.6. 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-communicatiemid-delen

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 (zakelijk en privé) 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, zoals 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. De organisatie zal de toegang tot andere e-maildiensten niet blokkeren of specifiek monitoren.

4.5. 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 de leidinggevende toegang tot de bestanden of mailbox van de medewerker te verschaffen doch uitsluitend nadat hiertoe expliciet toestemming van het College van Bestuur is verkregen en dit vervolgens kenbaar is gemaakt aan de betreffende medewerker. De leidinggevende 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 leidinggevende toegang krijgt.

Artikel 4, vijfde lid is ter goedkeuring voorgelegd aan de OR (artikel 27, lid 1, sub k WOR).

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 op inhoud 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 (zakelijk en privé) 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 weet of kan vermoeden 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. 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 platformen (zoals Facebook, Youtube, Instagram, Skype, Twitter of Linkedin). 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. Medewerker zal geen deelnemers toevoegen als ‘vrienden’ of contacten op dergelijke sociale media, tenzij hij interne social media platformen gebruikt (zoals Skype).

6.3. 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.

6.4. Dit artikel geldt ook indien de medewerker vanaf privécomputers of privéinternetaansluitingen gebruik maakt van sociale media, doch uitsluitend voor zover het gaat om deelname die het werk kan raken.

6.5. Wanneer de medewerker een extern sociale-media-account opzet dat direct werkgerelateerd is, terwijl het op naam van de medewerker persoonlijk is gesteld, zullen de 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 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 ICT-middelen wordt zo veel mogelijk langs technische weg onmogelijk gemaakt.

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 gegevens kunnen tot nadere technische maatregelen besluiten.

7.3. De Instelling houdt zich bij het controleren op het niveau van verkeersgegevens of persoonsgegevens onverkort aan de relevante wet- en regelgeving (zoals de Algemene verordening gegevensbescherming). In het bijzonder beveiligt de Instelling de bij controle vastgelegde gegevens tegen ongeautoriseerde toegang en zijn personen met toegang daartoe contractueel verplicht tot geheimhouding.

7.4. Enkele specifieke maatregelen ter controle die de Instelling kan uitvoeren, 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.

7.5 Uitsluitend bij een ernstig vermoeden van (grove) schending van de onderhavige gedragsregels kan in opdracht van het College van Bestuur op het niveau van individuele verkeersgegevens van het e-mail- en internetgebruik controle op inhoud worden uitgevoerd.

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 concrete aanwijzing of ernstig vermoeden van overtreding van dit Reglement door die medewerker.

8.2. Gericht onderzoek vindt uitsluitend plaats na schriftelijke opdracht van het College van Bestuur na advies van de afdeling juridische zaken. Het College van Bestuur ontvangt een afschrift van de resultaten van het onderzoek. Indien het onderzoek geen aanleiding geeft tot verdere maatregelen wordt de verslaglegging 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 het College van Bestuur 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 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 vastlegging wordt onder naam van het College van Bestuur 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 College van 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 het College van Bestuur 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. Beheerders (ICT medewerkers) 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. Consequenties van overtreding

9.1. Bij handelen in strijd met dit Reglement of de algemeen geldende wettelijke regels, kan het College van Bestuur afhankelijk van de aard en de ernst van de overtreding op grond van plichtsverzuim disciplinaire maatregelen treffen. Daarnaast kan het College van Bestuur besluiten tot een al dan niet tijdelijke beperking tot de toegang van bepaalde ICT-faciliteiten.

9.2. Disciplinaire maatregelen kunnen niet worden getroffen enkel op basis van een langs geautomatiseerde uitgevoerde verwerking van persoonsgegevens, zoals een constatering van een automatisch filter of blokkade. Vorenstaande geldt niet voor een waarschuwing (niet zijnde een disciplinaire maatregel).

9.3. 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.

Artikel 10. Slotbepaling

10.1. Dit Reglement treedt in werking per 1 augustus 2018. De ondernemingsraad en de gemeenschappelijke medezeggenschapsraad hebben op 5 juli 2018 ingestemd met artikel 7 en 8 van dit reglement. Wijzigingen worden alleen ingevoerd nadat ondernemingsraad en gemeenschappelijke medezeggenschapsraad hiermee hebben ingestemd.
10.2 In gevallen waarin dit Reglement niet voorziet, beslist het College van Bestuur.
10.3 Dit Reglement komt ter vervanging van de ICT gedragscode voor medewerkers