Acceptable Use Policy werknemers HZ

Reglement voor ICT- en internetgebruik voor werknemers aan HZ University of Applied Sciences

Acceptable Use Policy voor werknemers van HZ University of Applied Sciences

Basis voor het reglement

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

Met dit Reglement wil de instelling, HZ University of Applied Sciences, 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 en de privacy van de werknemer.

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.

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. Dit Reglement is naast de wet ook gebaseerd op de CAO HBO.

Artikel 1. Uitgangspunten

1.1. Het Reglement stelt regels ten aanzien van het gebruik van de bedrijfsmiddelen ICT en internet door werknemers. 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 werknemers, en van studenten en ouders;
- bescherming van vertrouwelijke informatie van de Instelling en haar werknemers, 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. Beperkt privégebruik van internet en ICT-middelen is alleen toegestaan tijdens pauzes en/of voor zover het werk er niet onder lijdt. Gebruik voor nevenwerkzaamheden is te allen tijde verboden tenzij aparte schriftelijke toestemming daarvoor is verkregen.

1.3. Dit Reglement geldt voor een ieder die voor de Instelling werkzaam is, dus ook voor uitzendkrachten en tijdelijke werknemers. Het Reglement geldt niet voor (gast)studenten; hiervoor is het aparte Studentenreglement opgesteld.

1.4. Dit Reglement geldt ook indien u als gast gebruik maakt van netwerkvoorzieningen van andere instellingen waarbij toegang wordt verkregen op basis van de inloggegevens van de eigen Instelling (Eduroam).

1.5. De Instelling streeft in het kader van handhaving van dit Reglement naar maatregelen die

inzage in privacygevoelige informatie of persoonsgegevens van individuele werknemers 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. De werknemer 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. De werknemer maakt geen inbreuk op de intellectuele eigendomsrechten van de Instelling en derden en respecteert de licentie afspraken zoals die van toepassing zijn binnen de Instelling.

2.3. De zeggenschap over de informatie van de Instelling berust bij Instelling. De werknemer heeft geen zelfstandige zeggenschap over de informatie behalve als hem dat expliciet is toegekend door de Instelling.

2.4. De werknemer 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 en de bescherming van intellectueel eigendom voorschriften heeft opgesteld zal werknemer deze strikt naleven.

2.5. Deze bepalingen gelden in het bijzonder voor medewerkers van de Dienst Informatievoorziening en Automatisering, voor wie schending van deze bepalingen als een zeer ernstig plichtsverzuim wordt aangemerkt, gezien hun bijzondere positie.

Artikel 3. Gebruik van computer- en netwerkfaciliteiten

3.1. Computer- en netwerkfaciliteiten worden aan de werknemer voor gebruik in het kader van zijn functie beschikbaar gesteld. 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 werknemer 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 het systeembeheer per direct het betrokken account ontoegankelijk maken.

3.3. De Instelling kan voor onderwijs- en andere bedrijfsdoeleinden systemen of applicaties voorschrijven, zoals een Elektronische Leeromgeving, een e- mailsysteem, (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. Het aansluiten van servers en actieve netwerkcomponenten (zoals access points en routers) is niet toegestaan zonder toestemming van de Dienst Informatievoorziening en Automatisering. De dienst kan aan de toestemming regels verbinden ter handhaving van dit reglement, zoals het moeten installeren van virusscanners en wachtwoordbeveiliging.

3.5. Het aansluiten van eigen client-apparatuur (zoals, laptops, tablets en telefoons) is alleen toegestaan op de daarvoor beschikbaar gestelde (wireless) netwerkaansluitingen. De Dienst Informatievoorziening en Automatisering kan aan de toegang tot deze aansluitingen regels verbinden ter handhaving van dit reglement, zoals het moeten installeren van virusscanners en wachtwoordbeveiliging.

3.6. 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.

3.7. Het gebruik van computer- en netwerkfaciliteiten door de werknemer 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 e-mailadres wordt aan de werknemer 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 te versturen of kwaadaardige software zoals virussen, Trojaanse paarden of spyware te versturen.

4.4. De werknemer gebruikt voor privé e-mail 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 grove nalatigheid van de werknemer, 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 werknemer te verschaffen, doch uitsluitend nadat hiertoe aparte toestemming van het College van Bestuur is verkregen. 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 / bedrijfsarts / personeelsadviseur. Indien de werknemer dergelijke markeringen niet heeft aangebracht, kan de Instelling door inschakeling van een vertrouwenspersoon de betreffende informatie van de werknemer controleren om zo privé informatie te herkennen en apart te plaatsen alvorens de vervanger of leidinggevende toegang krijgt.

4.6. E-mailberichten van leden van het medezeggenschapsorgaan onderling, van bedrijfsartsen, van personeelsadviseurs 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.

4.7. De werknemer gaat akkoord met het door applicaties van de Instelling geautomatiseerd plaatsen van kopieën van berichten die zijn vastgelegd door middel van deze applicaties in de e-mailbox en agenda van de werknemen in het e-mail systeem van de Instelling.

Artikel 5 Gebruik van internet

5.1. De toegang tot internet en bijbehorende faciliteiten worden aan de werknemer 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- of streamingdiensten 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 werknemer 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.
- volgens het wetboek illegale activiteiten te ontplooien op het HZ netwerk

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 werknemer met vakgenoten en derden via sociale media. Indien dit werk gerelateerde onderwerpen betreft, dient de werknemer ervoor te zorgen dat het profiel en de inhoud in overeenstemming is met hoe hij zich in tekst, beeld en geluid zou presenteren ten overstaan van collega's en studenten.

6.2. 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 werknemers lezen wat zij schrijven.

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

6.4. Wanneer werknemer een sociale-media-account opzet dat direct werk gerelateerd is, terwijl het op naam van werknemer persoonlijk is gesteld, zullen werknemer 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 bedrijfsmiddelen 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 medewerkers van de Dienst Informatievoorziening en Automatisering 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 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. Enkele specifieke maatregelen ter controle die de Instelling kan voeren, zijn:

- controle ter voorkoming van negatieve publiciteit en ongewenst gedrag, in het bijzonder van 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. Van gericht onderzoek is sprake wanneer verkeersgegevens of andere persoonsgegevens betreffende een specifieke werknemer worden vastgelegd in het kader van een onderzoek naar aanleiding van een zwaarwegend vermoeden van een overtreding van dit Reglement door die werknemer.

8.2. Gericht onderzoek vindt uitsluitend plaats na schriftelijke opdracht van het College van Bestuur. 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 het systeembeheer 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 werknemer 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.

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 werknemer wordt zo spoedig mogelijk schriftelijk geïnformeerd door of namens het College van Bestuur over de aanleiding, de uitvoering en het resultaat van het onderzoek. De werknemer wordt in de gelegenheid gesteld uitleg te geven over de aangetroffen gegevens. Uitstel van het informeren mag alleen als informeren het onderzoek daadwerkelijk zou schaden.

8.7. Medewerkers van de Dienst Informatievoorziening en Automatisering verschaffen zich slechts toegang tot accounts of computers van werknemers als de werknemer 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 werknemer zal in dat geval achteraf worden geïnformeerd.

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

9.1. De werknemer kan zich tot het bestuur wenden met het verzoek voor een volledig overzicht van zijn persoonsgegevens zoals door de Instelling verwerkt in het kader van dit Reglement. Aan een dergelijk verzoek wordt binnen vier weken voldaan.

9.2. De werknemer kan het bestuur verzoeken zijn persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen indien deze feitelijk onjuist zijn, voor het doel onvolledig of niet ter zake dienend zijn, dan wel in strijd met een wettelijk voorschrift zijn. Op een dergelijk verzoek wordt binnen vier weken gereageerd. Een weigering is met redenen omkleed. Een toegewezen verzoek zal zo spoedig mogelijk worden uitgevoerd.

9.3. De werknemer kan verder verzet aantekenen tegen de verwerking van zijn persoonsgegevens in verband met zwaarwegende persoonlijke omstandigheden. Het bestuur oordeelt binnen vier weken na ontvangst van het verzet of dit gerechtvaardigd is. Indien het bestuur het verzet gerechtvaardigd acht, beëindigt zij terstond de verwerking.

9.4. Het bestuur zal de werknemer geen opdrachten of dienstbevelen geven ten aanzien van privacygevoelige informatie en persoonsgegevens die in strijd zijn met dit Reglement.

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