# Gebruiksreglement ICT-voorzieningen voor medewerkers HKU

*Geldend vanaf 1 september 2014*

**INHOUD**

**INLEIDING**



**INLEIDING**

Het gebruik van internet en ICT-middelen is voor (veel van) de medewerkers binnen de instelling noodzakelijk om hun werk goed te kunnen doen. Hiertoe stelt de hogeschool ICT-voorzieningen beschikbaar die gebruikt worden in het kader van onderwijs, onderzoek en bedrijfsvoering. Aan het gebruik hiervan zijn echter risico's verbonden waardoor het stellen van gedragsregels nodig is. Tegen de achtergrond van deze risico's mag van de medewerkers verantwoord gebruik van internet en ICT worden verwacht.

Met dit reglement wil HKU, hierna te noemen "de instelling" regels stellen omtrent het gewenst gebruik van deze voorzieningen. Het streven daarbij is een goede balans aan te brengen tussen verantwoord en veilig ICT-gebruik en de privacy van de medewerker. Uitgangspunt hierbij is dat gebruikers de algemeen maatschappelijke normen en waarden respecteren en het gebruik van ICT-voorzieningen in lijn moet zijn met de onderwijs-, onderzoeks- of de bedrijfsvoering van de instelling.

**Artikel 1 Uitgangspunten**

1. DIt Reglement stelt regels ten aanzien van het gebruik van de ICT-voorzieningen 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 persoonsgegevens van medewerkers, van studenten en van relaties van de instelling;
   • bescherming van vertrouwelijke informatie van de instelling;
   • 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.
2. Beperkt privégebruik van internet en ICT-middelen is toegestaan, mits dit niet storend is voor de dagelijkse werkzaamheden of het netwerk van de instelling. Gebruik voor nevenwerkzaamheden is te allen tijde verboden tenzij aparte schriftelijke toestemming daarvoor is verkregen.
3. Dit Reglement geldt voor eenieder 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.
4. Dit Reglement geldt ook indien u als gast gebruik maakt van (netwerk-) voorzieningen van andere instellingen waarbij toegang wordt verkregen op basis van de inloggegevens van de eigen instelling bijvoorbeeld (Eduroam en/of SURFConext).
5. 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**

1. De medewerker dient vertrouwelijke 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. De medewerker maakt geen inbreuk op de intellectuele eigendomsrechten van de instelling en derden en respecteert de licentieafspraken zoals die van toepassing zijn binnen de instelling.
3. De zeggenschap over de informatie van de instelling berust bij de instelling. De medewerker heeft geen zelfstandige zeggenschap over de informatie behalve als hem dat expliciet is toegekend door de Instelling.
4. De medewerker besteedt bijzondere aandacht aan het treffen van maatregelen, 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 cloudtoepassingen (dropbox e.d.), op externe opslagmedia of eigen client-apparatuur (USB-apparaten, tablets, smartphones etc.).
5. Dit artikel geldt in het bijzonder voor systeem- en netwerkbeheerders, voor wie schending van dit artikel als een zeer ernstig plichtsverzuim wordt aangemerkt, gezien hun bijzondere positie.

**Artikel 3 Gebruik van computer- en netwerkfaciliteiten**

1. Computer- en netwerkfaciliteiten 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. Privégebruik is alleen toegestaan zoals bepaald in artikel 1.2.
2. De medewerker dient te allen tijde zorgvuldig om te gaan met aan hem persoonlijk toegekende inloggegevens en eventuele aanvullende authenticatiemiddelen. 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. De instelling kan voor onderwijs- en bedrijfsdoeleinden systemen of applicaties voorschrijven, zoals digitale studiepuntenadministratie, een e-mailsysteem, (mobiele) applicaties (apps), cloudvoorzieningen of multimediadiensten. De medewerker zal ten behoeve van onderwijs- en onderzoekstaken de voorgeschreven systemen gebruiken en de daarbij gestelde beperkingen en eisen stipt naleven.
4. Het installeren van software op de server- en netwerkfaciliteiten van de organisatie (anders dan in het gebruikersaccount) is niet toegestaan zonder aparte toestemming van het systeembeheer. Ook het aansluiten van servers en actieve netwerkcomponenten (zoals access points en routers is niet toegestaan zonder toestemming van het systeembeheer. Het systeembeheer kan aan de toestemming regels verbinden ter handhaving van dit reglement, zoals het moeten installeren van virusscanners en aanvullende wachtwoordbeveiliging. Het aansluiten van eigen client-apparatuur (zoals, laptops, tablets en telefoons) is alleen toegestaan op de daarvoor beschikbaar gestelde (wireless) netwerkaansluitingen. Het systeembeheer kan aan de toegang tot deze aansluitingen regels verbinden ter handhaving van dit reglement, zoals het moeten installeren van virusscanners en wachtwoordbeveiliging.
5. Het gebruik van computer- en netwerkfaciliteiten door de medewerker ten behoeve van nevenwerkzaamheden is uitsluitend toegestaan als en voorzover de instelling hiervoor schriftelijk toestemming heeft verleend.

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

1. Het e-mailsysteem en de bijbehorende mailbox, gebruikersaccount en 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.
2. Uitdrukkelijk verboden bij elk gebruik van ICT-communicatiemiddelen is:
   • het verzenden van berichten of het publiceren van webpagina's met een pornografische, racistische, discriminerende, bedreigende, beledigende of aanstootgevende inhoud;
   • het verzenden van berichten of het publiceren van webpagina's met een (seksueel) intimiderende inhoud;
   • het verzenden van berichten of het publiceren van webpagina's 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.
   • het publiceren of 'hosten' van kwaadaardige en/ of illegale software zoals mal- en spyware via het medewerkersaccount
   • het verzenden van berichten of het publiceren van informatie via websites, blogs e.d die de instelling en/ of zijn medewerkers, studenten en andere betrokkenen op enige wijze mogelijk kunnen schaden.
3. De medewerker gebruikt voor privémail bij voorkeur niet het door de instelling verstrekte e-mailadres, binnen de grenzen van artikel 1.2. De organisatie zal de toegang tot andere e-maildiensten niet blokkeren of specifiek monitoren.
4. In geval van ziekte, onverwacht langdurige afwezigheid of nalatigheid van de medewerker, is de instelling gerechtigd na toestemming van de medewerker een vervanger of leidinggevende

toegang tot het gebruikersaccount of mailbox van de medewerker te verschaffen. Indien aangetoond kan worden dat toestemming van de medewerker verkrijgen onmogelijk is of het bedrijfsbelang zodanig zwaar is dat toestemming niet gevergd kan worden, mag het College van Bestuur toestemming geven toegang te verschaffen tot de bestanden en mailbox in het gebruikersaccount.

5. E-mailberichten van en naar leden van het medezeggenschapsorgaan, van en naar bedrijfsartsen, van en naar vertrouwenspersonen, studentendecanen, P&O adviseurs, de ombudsman en van en naar eenieder 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**

1. De toegang tot internet en bijbehorende faciliteiten 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.
2. Ieder gebruik van internet en internetfaciliteiten moet binnen de grenzen van de wet plaatsvinden en in lijn zijn met de uitgangspunten van dit reglement. Uitdrukkelijk verboden is dan ook het gebruik van internet en netwerk faciliteiten in strijd met het Reglement goede gang van zaken, de Integriteitscode HKU en andere algemene en wettelijke normen betreffende de goede orde en veiligheid.

**Artikel 6 Gebruik van sociale media**

1. HKU 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, Google+, Skype, Twitter of LinkedIn). Indien dit werkgerelateerde onderwerpen betreft, dient de medewerker ervoor te zorgen dat het profiel en de inhoud in overeenstemming zijn met hoe hij zich in tekst, beeld en geluid zou presenteren ten overstaan van collega's en studenten.
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 medewerkers lezen wat zij schrijven.
3. 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.
4. Wanneer een medewerker een sociale-media-account opzet dat direct werkgerelateerd is, terwijl het op naam van 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**

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 zoveel mogelijk langs technische weg onmogelijk gemaakt.
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.
3. Bij vermoedens van overtreding van regels kan controle worden uitgevoerd op het niveau van individuele verkeersgegevens van het e-mail- en internetgebruik.

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.
5. 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 vinden plaats op basis van filtering van de inhoud op trefwoorden of inhoudelijke controle op basis van klachten of meldingen van derden;
   • 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.
6. Bij (geautomatiseerde) constatering van overlast kan de instelling een tijdelijke blokkade van de betreffende faciliteit invoeren. Deze blokkade zal zolang worden gehandhaafd tot aangetoond is dat de oorzaak is weggenomen.

**Artikel 8 Procedure bij gericht onderzoek**

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 vermoeden van een overtreding van dit reglement door die medewerker.
2. Gericht onderzoek vindt uitsluitend plaats na schriftelijke opdracht van een directeur van het onderdeel waar de betreffende medewerker taken verricht, ofwel door het College van Bestuur. 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.
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 medewerker met het doel de beveiliging of integriteit van de randapparatuur te verbeteren. Bij herhaling zal de procedure uit lid 2 worden gevolgd.
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.
5. 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 schaden.
6. 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, te bepalen door de directeur waar de medewerker taken verricht, het CvB, 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.

7. 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 disciplinaire maatregelen treffen conform hoofdstuk P van de Collectieve Arbeidsovereenkomst HBO. Indien sprake is van een misdrijf of overtreding, zal aangifte worden gedaan bij de politie.

**Artikel 9 Slotbepalingen**

1. HKU kan dit reglement wijzigen als de omstandigheden daar aanleiding toe geven. Voorgenomen wijzigingen worden voorafgaand aan de invoering aan de medewerkers bekend gemaakt.
2. In gevallen waarin dit reglement niet voorziet, beslist het College van Bestuur.

*Vastgesteld door het College van Bestuur d.d. 8 september 2014*