Reglement computergebruik medewerkers Open Universiteit

Basis voor dit reglement

Het gebruik van internet en ict-faciliteiten is voor het merendeel van de medewerkers binnen de Open Universiteit (OU) 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 medewerkers verantwoord gebruik van internet en ict-faciliteiten worden verwacht.

Met dit reglement wil de OU regels stellen omtrent het gewenst gebruik van deze bedrijfsmiddelen. Het streven daarbij is een goede balans aan te brengen tussen enerzijds verantwoord en veilig gebruik van internet en ict-faciliteiten en anderzijds de privacy van de medewerker.

Het gebruik van social media zoals Facebook, LinkedIn en X wordt steeds belangrijker maar kan ook zijn weerslag hebben op de OU. Daarom wil de OU ook hier bepaalde regels aan stellen.

De OU 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 hoofdstuk 6 van de CAO Nederlandse Universiteiten.

Omdat het reglement voorziet in een verwerking van persoonsgegevens en/of controle op gedrag of prestaties van medewerkers heeft de Ondernemingsraad instemmingsrecht.

Inhoudsopgave

Artikel 1. Definities

In dit reglement wordt verstaan onder:

a. Bijzondere persoonsgegevens
Persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en strafrechtelijke persoonsgegevens.

b. CERT OU
Het Computer Emergency Response Team van de OU, zoals beschreven in het Operationeel model van CERT OU. De FG is lid van CERT OU. Het team neemt meldingen over informatiebeveiligingsincidenten in ontvangst en bewaakt de afhandeling daarvan.

c. Directeur ITF
De directeur ITF is verantwoordelijk voor het beschikbaar stellen van ict-faciliteiten. De directeur is bevoegd uitvoeringsregels vast te stellen binnen de kaders van dit reglement. Deze uitvoeringsregels kunnen aan alle gebruikers van de ict-faciliteiten beperkingen opleggen bij de toepassing van deze faciliteiten.

d. ITF
Het organisatieonderdeel van de OU dat ict-faciliteiten ter beschikking stelt en medewerkers ondersteunt bij het gebruik daarvan.

e. Functionaris Gegevensbescherming (FG)
Door het College van bestuur benoemde en bij de Autoriteit Persoonsgegevens geregistreerde toezichthouder op de toepassing en naleving van de privacywetgeving zoals bedoeld in de Algemene Verordering Gegevensbescherming (AVG).

f. Gebruik voor privé doeleinden
Het gebruik van ict-faciliteiten anders dan voor direct werkgerelateerde doeleinden.

g. Gericht onderzoek
Een activiteit waarbij verkeersgegevens of andere (persoons)gegevens betreffende c.q. van een specifieke medewerker worden verzameld in het kader van een onderzoek naar aanleiding van een zwaarwegend vermoeden van een overtreding van dit Reglement door die medewerker.

h. Ict-faciliteiten
De door of namens de OU ter beschikking gestelde ict-apparatuur, programmatuur, al dan niet draadloze toegang tot het netwerk alsmede voorzieningen voor elektronische informatie-uitwisseling. Deze omschrijving is niet limitatief.

i. Leidinggevende
De decaan of directeur die eindverantwoordelijk is voor een faculteit resp. dienst.

j. Medewerker
Iedere vaste of tijdelijke medewerker, gedetacheerde, stagiaire of externe opdrachtnemer van de OU en overige derden die gebruik maken van de ict-faciliteiten van de OU.

k. Nevenwerkzaamheden
Alle werkzaamheden en activiteiten die een werknemer buiten de opgedragen taak bij de universiteit verricht, ongeacht:
   a. de omvang van het dienstverband bij de OU
   b. de omvang van de nevenwerkzaamheden
   c. of de werknemer een beloning ontvangt voor de nevenwerkzaamheden
   d. de werkzaamheden buiten of binnen werktijd worden verricht.

l. Verkeersgegevens
Gegevens (meta-data) betreffende elektronische berichten die door medewerkers worden verstuurd en ontvangen. Het betreft niet de inhoud van die berichten maar alleen de volgende gegevens:
- adressen van afzender en ontvanger;
- datum en tijdstip van versturen en ontvangen van het bericht;
- grootte in bytes van het bericht;
- adres van de werkplek of server van de afzender;
- statusinformatie m.b.t. het afleveren (bv. afgeleverd of in wachtrij geplaatst).

m. Vertrouwenspersoon computergebruik
Een medewerker van de OU die de privacybelangen van een andere medewerker behartigt indien die belangen tijdelijk moeten worden geschonden in het belang van de OU en met toestemming van de FG. Deze vertrouwenspersoon computergebruik wordt door de FG per geval aangewezen.

Artikel 2. Algemeen doel en reikwijdte

1. Doel van dit reglement is de goede orde te bepalen ten aanzien van:

   a) systeem- en netwerkbeveiliging, inclusief beveiliging tegen schade en misbruik;
   b) tegengaan van seksuele intimidatie, discriminatie en andere strafbare feiten;
   c) bescherming van privacy gevoelige informatie waaronder persoonsgegevens die door de OU worden verwerkt;
   d) bescherming van vertrouwelijke informatie van de OU, haar medewerkers en haar studenten;
   e) bescherming van de intellectuele eigendomsrechten van de OU en derden waaronder het respecteren van de licentie-afspraken die van toepassing zijn binnen de OU;
   f) voorkomen van negatieve publiciteit;
   g) kosten- en capaciteitsbeheersing;
   h) het creëren van een basis waarop kan worden opgetreden tegen verboden gebruik;
   i) voorkomen dat de continuïteit van het primaire proces van de OU in gevaar komt en dat het gebruik van de ict-faciliteiten in strijd is met de primaire doelstelling van de OU.

2. Het is medewerkers toegestaan om de ict-faciliteiten te gebruiken voor privédoeleinden, tenzij dit gebruik ernstige inbreuk maakt op de productieve arbeidsuren en/of de kwaliteit van het werk aantast.

3. Het is medewerkers niet toegestaan om zodanig excessief gebruik te maken van ict-faciliteiten, of een dergelijk gebruik door anderen uit te lokken, dat de bedrijfsprocessen van de OU daar hinder van ondervinden.

4. Gebruik van de ict-faciliteiten voor nevenwerkzaamheden is te allen tijde verboden tenzij aparte schriftelijke toestemming daarvoor is verkregen.

5. Dit reglement geldt ook indien medewerkers van de OU als gast gebruik maken van netwerkvoorzieningen van andere instellingen, waarbij toegang wordt verkregen op basis van de inloggegevens van de OU (eduroam).

6. De OU 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. De OU zal waar mogelijk slechts geautomatiseerd controleren of filteren zonder daarbij iemand inzage te geven in gedrag van individuele personen.

7. Op het gebruik van ict-faciliteiten is tevens de Algemene Verordening Gegevensbescherming s van toepassing waarin als voorwaarden voor het rechtmatig verwerken van persoonsgegevens zijn genoemd:

   a) Rechtmatigheid, behoorlijkheid en transparantie;
   b) Doelbinding;
   c) Dataminimalisatie;
   d) Juistheid;
   e) Opslagbeperking;
   f) Vertrouwelijkheid en integriteit;

8. Passende technische en organisatorische maatregelen zijn getroffen teneinde de persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.

Artikel 3. Intellectueel eigendom en vertrouwelijke informatie

1. De medewerker dient vertrouwelijke informatie – waaronder privacygevoelige informatie zoals 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 OU en derden en respecteert de licentie afspraken zoals die van toepassing zijn binnen de OU.

3. Bij de verwerking van vertrouwelijke informatie buiten de OU besteedt de medewerker bijzondere aandacht aan het treffen van maatregelen om de vertrouwelijkheid te waarborgen. Onder verwerking buiten de OU wordt onder meer verstaan: versturen via e-mail, verwerken in niet instellingsgebonden cloud-toepassingen, op externe opslagmedia of (eigen) client-apparatuur (smartphones, USB-apparaten, tablets, etc.). Verwerken buiten de OU is slechts toegestaan indien dit in het kader van het uitvoeren van de werkzaamheden noodzakelijk is. De medewerker zal daarbij de voorschriften met betrekking tot het waarborgen van de vertrouwelijkheid – waaronder het Privacy reglement en het Informatiebeveiligingsbeleid – strikt naleven.

4. Medewerkers die uit hoofde van hun functie zodanige toegangsrechten hebben dat zij zich toegang kunnen verschaffen tot niet openbare informatie waarvan zij niet de eigenaar zijn, verschaffen zich slechts toegang tot die informatie als de eigenaar van de informatie daarvoor zijn toestemming heeft gegeven. Toegang zonder de toestemming van de eigenaar is slechts toegestaan in opdracht van de FG. Voor de in dit lid bedoelde medewerkers wordt schending van deze bepalingen als een zeer ernstig plichtsverzuim aangemerkt, gezien hun bijzondere positie.

Artikel 4. Gebruik van Ict-faciliteiten

1. Ict-faciliteiten worden aan de medewerker beschikbaar gesteld 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 2, leden 2 tot en met 5.

2. De door de OU verstrekte gebruikersnamen en authenticatiemiddelen (zoals wachtwoorden, certificaten, verificatiecodes en tokens) zijn persoonlijk. Het is medewerkers niet toegestaan om hun authenticatiemiddelen aan een ander beschikbaar te stellen. Het is niet toegestaan om zich met andere dan de persoonlijk toegekende gebruikersnamen toegang te verschaffen of pogingen te ondernemen andere gebruikersnamen te verkrijgen. Bij een vermoeden van misbruik van een gebruikersnaam kan het hoofd ITF-O per direct de betrokken gebruikersnaam ontoegankelijk maken.

3. Het aansluiten van servers en actieve netwerkcomponenten (zoals access points en routers) is niet toegestaan zonder toestemming van het Hoofd ITF-O. Het Hoofd ITF-O kan aan de toestemming regels verbinden ter handhaving van dit reglement, zoals het installeren van virusscanners en het toepassen van authenticatie.

4. Het aansluiten van eigen client-apparatuur (zoals laptops, tablets en smartphones) is alleen toegestaan op de daarvoor beschikbaar gestelde (wireless) netwerkaansluitingen. Het Hoofd ITF-O kan aan de toegang tot deze aansluitingen regels verbinden ter handhaving van dit reglement, zoals het installeren van virusscanners en het toepassen van authenticatie.

5. Het opslaan van privébestanden of -informatie op systemen van de OU 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 OU is echter niet verplicht reservekopieën van dergelijke bestanden of informatie beschikbaar te stellen.

6. Het gebruik van computer- en netwerkfaciliteiten door de medewerker ten behoeve van nevenwerkzaamheden is uitsluitend toegestaan als en voor zover de OU hiervoor cf. 4 schriftelijk toestemming heeft verleend.

7. Het is niet toegestaan bijzondere persoonsgegevens van een ander op te slaan. Het opslaan van overige persoonsgegevens via ict-faciliteiten is slechts toegestaan voor zover dit rechtmatig geschied en de bescherming van de persoonlijke levenssfeer van de persoon op wie de gegevens betrekking hebben zich hiertegen niet verzet.

Artikel 5. Gebruik van e-mail

1. Het e-mailsysteem en de bijbehorende mailbox 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. Privégebruik van deze middelen is alleen toegestaan zoals bepaald in Artikel 2, leden 2 tot en met 5.

3. Verboden bij elk gebruik (privé of niet) van e-mail is echter:

    a) het verzenden van berichten met een pornografische, racistische, discriminerende, bedreigende, beledigende of aanstootgevende inhoud;

    b) het verzenden van berichten met een (seksueel) intimiderende inhoud;

    c) het verzenden van berichten die (kunnen) aanzetten tot discriminatie, haat en/of geweld;

    d) het versturen van ongevraagde berichten aan grote aantallen ontvangers, het versturen van kwaadaardige software zoals virussen of spyware;

    e) bijzondere persoonsgegevens te versturen. Het versturen van overige persoonsgegevens via ict-faciliteiten is slechts toegestaan voor zover de bescherming van de persoonlijke levenssfeer van de persoon op wie de gegevens betrekking hebben zich hiertegen niet verzet. Het is aan medewerkers die toegang hebben tot hoofdstuk 6.2 (ziekte) van het personeelsdossier van een medewerker wel toegestaan om mededeling te doen van gegevens betreffende de gezondheid van die medewerker, voor zover dit noodzakelijk is voor:

f) een goede uitvoering van wettelijke voorschriften, pensioenregelingen of collectieve arbeidsovereenkomsten die voorzien in aanspraken die afhankelijk zijn van de gezondheidstoestand van betrokkene, of

g) de re-integratie of begeleiding van medewerkers of uitkeringsgerechtigden in verband met ziekte of arbeidsongeschiktheid.

4. Medewerkers mogen e-mail berichten uitsluitend lezen als zij tot de geadresseerden van het bericht behoren. Bovendien mogen zij e-mail berichten lezen waarvan een van de geadresseerden hen daartoe aantoonbaar heeft gemachtigd.

5. Het is medewerkers niet toegestaan e-mail te versturen met als afzender of ondertekening het e-mailadres of de naam van een ander, zonder dat die ander hen daartoe aantoonbaar heeft gemachtigd.

6. Het inkomende en uitgaande e-mailverkeer van de OU wordt in het kader van systeem- en netwerkbeveiliging op geautomatiseerde wijze gecontroleerd op virussen en andere schadelijke programma's. Besmette e-mail wordt vernietigd.

7. Het inkomende en uitgaande e-mailverkeer wordt op geautomatiseerde wijze gecontroleerd op spam.

   a) De inkomende berichten worden gemarkeerd met het gemeten spam niveau. Alle inkomende berichten worden bezorgd bij de geadresseerde, die zelf kan besluiten hoe de spam te behandelen. Er wordt geen tot personen herleidbare informatie bewaard over de resultaten van dit proces.

   b) Bij de uitgaande berichten wordt op grond van de aantallen geadresseerden een spam niveau bepaald. In geval van twijfel worden de berichten vastgehouden tot is vastgesteld of de berichten alsnog verzonden moeten worden.

8. Het hoofd ITF-O kan een bovengrens vaststellen voor de aantallen geadresseerden van werkgerelateerde mailings. Voor mailings met een aantal geadresseerden hoger dan deze bovengrens, wordt een aparte procedure aangeboden.

Artikel 6. 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. Privégebruik van deze middelen is alleen toegestaan zoals bepaald in Artikel 2, leden 2 tot en met 5.

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

   a) sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten, tenzij het bezoeken van dergelijke sites noodzakelijk is voor onderwijs- of onderzoeksdoeleinden en hiervoor schriftelijke toestemming is verkregen van de verantwoordelijke leidinggevende;

   b) 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;

   c) gegevens ongeautoriseerd te verwijderen, te veranderen of in te zien;

d) films, muziek, software en overig auteursrechtelijk beschermd materiaal te downloaden wanneer de medewerker daadwerkelijk weet of redelijkerwijze kon weten dat dit in strijd met auteursrechten is;

e) films, muziek, software en overig auteursrechtelijk beschermd materiaal te verspreiden (uploaden) naar derden zonder toestemming van de rechthebbenden;

f) websites of andere informatie te onderhouden of aan te bieden t.b.v. nevenwerkzaamheden.

Artikel 7. Gebruik van social media

1. De OU ondersteunt de open dialoog en de uitwisseling van ideeën en het delen van kennis van de medewerker met vakgenoten en derden via social media (zoals Facebook, Youtube, MSN, Skype, Omegle, X 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. E.e.a. conform artikel 1.8, lid 3 van de CAO NU: Van de medewerker wordt verwacht dat hij bij de uitoefening van zijn functie en in zijn persoonlijke en gemeenschappelijke optreden naar buiten, naar vermogen in de geest van de doelstelling van de universiteit te werk gaat.

2. Bestuurders, leidinggevenden en anderen die namens de OU beleid of strategie uitdragen hebben een bijzondere verantwoordelijkheid bij het gebruik van social 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 social media, doch uitsluitend voor zover het gaat om deelname die het werk kan raken.

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

Artikel 8. Rechten van de medewerker m.b.t. persoonsgegevens

1. De medewerker kan zich tot het College van bestuur wenden met het verzoek voor een volledig overzicht van zijn persoonsgegevens zoals door de OU verwerkt. Aan een dergelijk verzoek wordt binnen vier weken voldaan.

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

3. De medewerker kan het College van 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.

4. Het College van bestuur zal de medewerker geen opdrachten of dienstbevelen geven ten aanzien van privacygevoelige informatie en persoonsgegevens die in strijd zijn met dit reglement.

Artikel 9. Toegang tot ict-faciliteiten van medewerkers in noodgevallen

In noodgevallen waarbij de continuïteit van werkzaamheden ten behoeve van de OU dient te worden gegarandeerd – waaronder ten minste wordt verstaan: overlijden, langdurige afwezigheid of ontslag op staande voet van een medewerker – kan een leidinggevende schriftelijk aan de FG verzoeken om relevante informatie uit de ict-faciliteiten van een van zijn medewerkers. De FG toetst of die informatie vereist is o.b.v. noodzakelijkheid en/of continuïteit van de bedrijfsvoering. Indien de FG beslist om die informatie te laten verstrekken aan de leidinggevende, wijst hij een vertrouwenspersoon computergebruik aan en geeft hij ITF opdracht om een nieuw wachtwoord toe te kennen aan de gebruikersnaam van de betreffende medewerker en dat wachtwoord aan de vertrouwenspersoon computergebruik mede te delen. De vertrouwenspersoon computergebruik:

1. Informeert de betreffende medewerker dat er informatie uit zijn ict-voorzieningen (waaronder eventueel e-mail berichten) aan diens leidinggevende zal worden verstrekt.

2. Werkt samen met de leidinggevende om hem de noodzakelijke informatie te verstrekken, waarbij de privacy en de andere belangen van de betreffende medewerker zo weinig mogelijk worden geschaad. Informatie die is uitgewisseld met medezeggenschapsorganen, bedrijfsartsen, HR-adviseurs e.d. wordt nooit aan de leidinggevende verstrekt.

3. Treft maatregelen om te verzekeren dat de informatievoorziening zo wordt aangepast dat de leidinggevende – ook bij voortdurende afwezigheid van de betreffende medewerker – over de relevante informatie kan beschikken. Denk hierbij aan het verstrekken van kopieën van relevante informatie en het in e-mail instellen van een automatisch antwoord bij afwezigheid om afzenders er op te attenderen de dat geadresseerde tijdelijk niet bereikbaar is.

4. Indien relevant verzoekt hij ITF om de ict-faciliteiten weer uitsluitend beschikbaar te maken voor de betreffende medewerker en informeert hij die medewerker over de getroffen maatregelen.

NB: Medewerkers kunnen voorkomen dat hun privacy en andere belangen bij een dergelijke ingreep worden geschaad door zo weinig mogelijk persoonlijke informatie in de ict-voorzieningen van de OU te bewaren en eventuele persoonlijke informatie en e-mail af te zonderen van de bedrijfsinformatie en die als persoonlijk te kenmerken.

Artikel 10. Monitoring en controle

1. Controle van gebruik van de internet en ict-faciliteiten vindt slechts plaats in het kader van handhaving van de regels uit dit reglement voor de doelen genoemd in Artikel 2. Verboden gebruik van de bedrijfsmiddelen wordt zo veel mogelijk langs technische weg onmogelijk gemaakt.

2. Met inachtneming van de Wet bescherming persoonsgegevens worden – ter voorkoming van beheer- en capaciteitsproblemen, ter voorkoming van misbruik van de faciliteiten en ten behoeve van controle op de naleving van de regels – geautomatiseerd verkeersgegevens verzameld (gelogd). Deze verkeersgegevens zijn alleen toegankelijk voor de direct verantwoordelijke systeembeheerders en de FG en worden alleen in geanonimiseerde vorm aan overige beheerders en andere verantwoordelijken beschikbaar gesteld. Deze kunnen tot nadere technische maatregelen besluiten. Eventuele andere gegevens die bij dit proces worden aangetroffen zullen door ITF-O niet worden gebruikt en niet worden bewaard.

3. Noodzakelijke loggings en/of back-ups van verkeersgegevens die door ITF zijn verzameld, worden niet openbaar gemaakt en niet langer bewaard dan noodzakelijk. Deze verkeersgegevens worden gebruikt om eventuele problemen te traceren.

Artikel 11. Procedure bij Gericht onderzoek

1. Klachten omtrent gebruik van ict-faciliteiten door een individuele medewerker kunnen door iedere medewerker worden gemeld bij de leidinggevende van de betreffende medewerker of – indien er sprake is van gebruik als bedoeld in 3.a) en 3.a) – aan de vertrouwenspersoon van de Klachtencommissie ongewenste omgangsvormen. Indien de klacht wordt ingediend bij de Klachtencommissie, wordt zij afgehandeld conform de voor deze commissie geldende procedure.

2. De leidinggevende van een medewerker ten aanzien van wie een klacht is ingediend als bedoeld in het voorgaande lid besluit of er een zwaarwegend belang aanwezig is en of gericht onderzoek omtrent het gebruik van ict-faciliteiten nodig is. Indien hij een gericht onderzoek nodig acht, vraagt hij zo spoedig mogelijk na ontvangst van de klacht advies aan de FG. Op basis van dit advies neemt de leidinggevende een besluit ten aanzien van het uit te voeren gericht onderzoek. De FG wijst een onderzoeker en een vertrouwenspersoon computergebruik aan om dit onderzoek uit te voeren. Het College van bestuur ontvangt onmiddellijk een afschrift van deze opdracht en na afloop van het onderzoek een vastlegging van de resultaten daarvan.

3. Gericht onderzoek beperkt zich in eerste instantie tot verkeersgegevens van het gebruik van de faciliteiten. Als gericht onderzoek nader bewijs oplevert, kan de OU 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. Het College van bestuur laat zich, alvorens hij een besluit neemt, adviseren door de FG en de verantwoordelijk leidinggevende.

4. Indien de OU overgaat tot een onderzoek van de inhoud van communicatie of opgeslagen bestanden, kan de OU o.a. de volgende specifieke persoonsgebonden maatregelen ter controle treffen:

   – controle op het uitlekken van vertrouwelijke informatie. Dit vindt plaats op basis van steekproefsgewijze controle op trefwoorden. Verdachte berichten of bestanden worden apart gezet voor nader onderzoek;

   – controle op overtreding van het verbod uit 3. Dit vindt plaats door op klacht (of steekproefsgewijs) e-mailberichten te openen en de inhoud te raadplegen.

5. Indien aanvullende expertise is vereist kan de FG interne dan wel externe deskundigen inschakelen.

6. Informatie die is uitgewisseld met medezeggenschapsorganen, bedrijfsartsen, HR-adviseurs e.d. wordt bij een Gericht onderzoek buiten beschouwing gelaten. Ook hier geldt dat medewerkers kunnen voorkomen dat hun privacy en andere belangen bij een dergelijke ingreep worden geschaad, door zo weinig mogelijk persoonlijke informatie in de ict-voorzieningen van de OU te bewaren en eventuele persoonlijke informatie en e-mail af te zonderen van de bedrijfsinformatie en die als persoonlijk te kenmerken.

7. Op de onderzoeker en op allen die bij het onderzoek worden ingeschakeld, rust een geheimhoudingsplicht ten aanzien van het in dit artikel beschreven Gericht onderzoek en eventuele resultaten daarvan. De FG zal de ingeschakelde medewerkers over deze geheimhoudingsplicht informeren.

8. Op de verwerking van persoonsgegevens in het kader van een Gericht onderzoek is de Wet bescherming persoonsgegevens van toepassing.

9. De werknemer wordt zo spoedig mogelijk na afronding van het Gericht onderzoek schriftelijk door de leidinggevende geïnformeerd 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. Eventuele consequenties bij geconstateerde overtredingen van dit reglement worden beschreven in Artikel 14.

10. De gegevens die in het kader van een Gericht onderzoek betreffende het gebruik van ict-faciliteiten worden verkregen worden bewaard door de FG. Deze gegevens worden slechts bewaard:

    a) gedurende de termijn die nodig is voor het afronden van het onderzoek en het eventueel nemen van maatregelen. Onder maatregelen wordt verstaan disciplinaire maatregelen met inachtneming van Hoofdstuk 6, paragraaf 2 van de CAO Nederlandse Universiteiten.

    b) alsmede in afwachting van het aantekenen en afhandelen van verzet als bedoeld in Artikel 13.

Artikel 12. Klachten van derden

1. In afwijking van de procedure neergelegd in Artikel 11 geldt een versnelde procedure wanneer de OU een klacht ontvangt van een derde met betrekking tot het gebruik van ict-faciliteiten van de OU.

2. Een klacht als bedoeld in het eerste lid dient door de ontvanger daarvan middels een e-mailbericht aan cert@ou.nl te worden doorgestuurd aan de FG. Derden kunnen hun klachten ook zelf richten aan voornoemd e-mailadres.

3. Indien de klacht gericht is op een persoon voert de FG een eerste onderzoek uit naar de aard van de klacht. Naar aanleiding van dit onderzoek bepaalt de FG of een nader onderzoek naar het gebruik van ict-faciliteiten noodzakelijk is en schakelt zo nodig de hulp van CERT OU in. Tevens stelt de FG de verantwoordelijk leidinggevende op de hoogte.

4. Indien de klacht is gericht op ict-faciliteiten (zoals apparatuur) dan schakelt de FG CERT OU in. CERT OU lost de klacht op – zo nodig met hulp van medewerkers van ITF-O en rapporteert aan de FG en aan de klager. Indien bij de oplossing het vermoeden rijst dat er toch sprake is van handelingen die in strijd zijn met dit reglement, dan meldt CERT OU dat feit aan de FG.

5. Indien van toepassing formuleert de FG een formele reactie aan de klager en adviseert de FG de verantwoordelijke leidinggevende met betrekking tot eventueel te nemen maatregelen ten opzichte van de medewerker(s) die de handeling waartegen de klacht is gericht heeft/hebben verricht.

6. De verantwoordelijke leidinggevende neemt eventuele maatregelen en rapporteert hierover – met inachtneming van de Wet bescherming persoonsgegevens – aan het College van bestuur.

Artikel 13. Verzet

1. De medewerker ten aanzien van wie een Gericht onderzoek is of wordt uitgevoerd kan daartegen verzet aantekenen bij het College van bestuur. De termijn om verzet aan te tekenen eindigt in ieder geval twee weken nadat de medewerker door de leidinggevende is geïnformeerd over de uitkomsten van het gericht onderzoek.

2. Indien de termijn voor het aantekenen van verzet is verstreken zonder dat verzet is aangetekend, worden de in het onderzoek verzamelde gegevens terstond vernietigd.

3. Het College van bestuur reageert binnen vier weken na ontvangst van het verzet. Indien het verzet als bedoeld in het voorgaande lid gegrond wordt verklaard, worden de door middel van het Gericht onderzoek verkregen gegevens terstond vernietigd. Tevens worden eventuele maatregelen die zijn genomen naar aanleiding van het nader onderzoek herroepen.

4. Een beslissing op verzet als bedoeld in het eerste lid van dit artikel geldt als een besluit in de zin van de Algemene wet bestuursrecht.

Artikel 14. Consequenties van overtreding

1. Medewerkers ten aanzien van wie geconstateerd is dat zij zich niet aan dit reglement houden, worden zo spoedig mogelijk door de leidinggevende op hun gedrag aangesproken. Zij krijgen daarbij inzage in de over hen vastgelegde gegevens en hebben de gelegenheid te reageren op het geconstateerde. Medewerker en leidinggevende maken dan afspraken voor de toekomst en de mogelijke sanctie(s) bij overtreding daarvan. Deze afspraken kunnen strenger zijn dan het in dit reglement bepaalde. Ook kan de toegang tot e-mail of internet worden beperkt of geheel worden afgesloten.

2. 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, zoals genoemd in artikel 6.12 van de CAO NU en het daarop gebaseerde vigerende reglement Disciplinaire maatregelen van de OU.

3. Disciplinaire maatregelen (behalve een waarschuwing) kunnen niet worden getroffen enkel op basis van een langs geautomatiseerde weg 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.

4. Indien de OU gedwongen wordt aan een derde een financiële vergoeding en/of boete te betalen omdat een medewerker de rechten van intellectuele eigendom zoals bedoeld in 3.c) van dit reglement heeft geschonden, zal de OU deze vergoeding en/of boete verhalen op de medewerker persoonlijk indien onomstotelijk vaststaat dat betreffende medewerker voornoemd artikel van dit reglement bewust heeft geschonden.

Artikel 15. Slotbepaling en onvoorziene omstandigheden

1. Het Reglement computergebruik medewerkers OU zal door of namens het College van bestuur tweejaarlijks worden geëvalueerd en voor zover nodig worden aangepast aan nieuwe ontwikkelingen in wet-, regelgeving en jurisprudentie dan wel in verband met maatschappelijke en/of technische ontwikkelingen.

2. Het College van bestuur kan dit reglement wijzigen als de omstandigheden daar aanleiding toe geven. Voorgenomen wijzigingen worden voorafgaand aan de invoering aan de medewerkers bekend gemaakt. Indien er sprake is van inhoudelijke aanpassingen wordt ook de Ondernemingsraad geraadpleegd.

3. In alle gevallen waarin dit reglement niet voorziet, beslist het College van bestuur.

Artikel 16. Inwerkingtreding

1. Dit Reglement computergebruik medewerkers OU is vastgesteld door het College van bestuur op 19 december 2023 met instemming van de Ondernemingsraad d.d. 14 december 2023.

2. Dit Reglement computergebruik medewerkers OU treedt in werking op 1 januari 2024.

3. Met de inwerkingtreding van dit Reglement computergebruik medewerkers OU vervalt de eerdere versie van het Reglement computergebruik medewerkers OU met kenmerk U2014/6201.

4. Dit reglement kan worden aangehaald als *Computerreglement medewerkers*.