Radboud Universiteit

Acceptable Use Policy voor werknemers

Gedragscode voor ICT- en internetgebruik voor medewerkers van de Radboud Universiteit

Auteur(s):	R.Sarelse CISO/FG

Versie:	2.2
Datum:	mei 2018

Versie	Datum	Korte beschrijving aanpassingen
1.0	januari 2017	Eerste versie gebaseerd op SURF AUP-model versie 4.0
2.0	februari 2018	Commentaar GV verwerkt
2.1	Maart 2018	Commentaar CvB verwerkt
2.2	Mei 2018	Commentaar GV verwerkt

Acceptable Use Policy

Dit document dient als gedragscode voor ICT- en internetgebruik van werknemers van de Radboud Universiteit, verder te noemen de Gedragscode.

Basis voor de gedragscode

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 deze Gedragscode wil de instelling, Radboud Universiteit, 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 sociale media wordt steeds belangrijker maar kan ook zijn weerslag hebben op de Instelling. Daarom wil de Instelling ook hier bepaalde regels aan verbinden.

De Instelling is als werkgever bevoegd regels te stellen omtrent de uitvoering van het werk en de goede orde op de werkvloer. De Gedragscode is naast de wet ook gebaseerd op de CAO NU.

Omdat de Gedragscode voorziet in een verwerking van persoonsgegevens en/of controle op gedrag of prestaties van werknemers, is het medezeggenschapsorgaan (OR) instemmings-plichtig. De OR heeft op 1 oktober 2018 ingestemd met de inhoud van deze Gedragscode.

1. Uitgangspunten

1.1. De Gedragscode 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 persoonsgegevens van de 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.

De instelling informatieveiligheidspolicy en andere informatie over informatieveiligheid en andere richtlijnen zijn beschikbaar op de RU's informatieveiligheidspagina's:

http://www.ru.nl/privacy

Specifieke IT-diensten of faciliteiten kunnen specifieke richtlijnen hebben die apart bekend worden gemaakt. Neem in geval van twijfel omtrent de richtlijnen en reglementen contact op met het lijn-management.

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

1.3. De Gedragscode geldt voor een ieder die voor de Instelling werkzaam is, dus ook voor uitzendkrachten en tijdelijke werknemers. Voor gasten van werknemers geldt de Gedragscode eveneens.

1.4. De Gedragscode 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 de Gedragscode naar maatregelen die inzage in privacygevoelige informatie of persoonsgegevens van individuele werknemers zo veel mogelijk beperken.

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 mag geen inbreuk maken 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 de Instelling. De werknemer heeft geen zelfstandige zeggenschap over de informatie behalve als hem dat expliciet is toegekend door de Instelling.[1]

2.4. Het is de werknemer niet toegestaan om systematisch grote hoeveelheden artikelen uit de bestanden van de digitale bibliotheek te downloaden of substantiële delen van de bestanden of databases in de digitale bibliotheek systematisch te kopiëren[2].

[1] Zie ook Algemene regels ten behoeve van Kennisbescherming en Kennisexploitatie van de Radboud Universiteit Nijmegen en het UMC St Radboud

[2] Bedoeld worden enorme aantallen die niet handmatig gedownload worden om te voorkomen dat de hele Radboud Universiteit afgesloten wordt van de toegang.

2.5. De werknemer 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. Delen via E-mail, opslag in niet instellingsgebonden Cloud-toepassingen, op externe opslagmedia of eigen client-apparatuur (USB-apparaten, Tablets, etc.) dient aan de door de RU vereiste voorwaarden te voldoen.
Indien de Instelling met betrekking tot het waarborgen van de vertrouwelijkheid voorschriften heeft opgesteld zal werknemer deze strikt naleven. Zie daarvoor www.ru.nl/privacy en www.radboudnet/privacy.

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

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 1.2.

3.2. De werknemer 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[3] 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 installeren van software op de niet persoonlijke computer[4]- en netwerkfaciliteiten van de organisatie 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 de Gedragscode, zoals het moeten installeren van virusscanners en 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

[3] Dit kan het ISC of een andere erkende RU ondersteuningsgroep zijn
[4] Pc's in vergaderruimtes, hal, gang, bibliotheek, refter, studiezalen etc.

regels verbinden ter handhaving van de Gedragscode, 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. Hiervoor is het gewenst dat prive gegevens in een submap met de naam 'prive' gescheiden worden van werkgegevens. 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. De persoonlijke U-schijf wordt als netwerkschijf wel geback-upt dus aangeraden in plaats van lokale opslag.

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 1.2.

4.3. Gebruik, privé of ten behoeve van studie, mag niet storend zijn voor de goede orde bij de Instelling en mag geen overlast veroorzaken bij anderen, inbreuk maken op rechten van de Instelling of derden of de integriteit en de veiligheid van het netwerk aantasten.

Onder storend en/of overlast veroorzakend gebruik wordt in ieder geval verstaan[5]

- 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 privémail bij voorkeur niet het door de Instelling verstrekte e-mail adres, binnen de grenzen van 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

[5] In zeer specifieke gevallen kan hiervan worden afgeweken, bijvoorbeeld bepaalde gedragingen die normaliter als storend worden ervaren, maar die noodzakelijk zijn in het kader van wetenschappelijk onderzoek.

tot de bestanden of mailbox van de werknemer te verschaffen doch uitsluitend indien aangetoond kan worden dat toestemming van de werknemer verkrijgen onmogelijk is of het bedrijfsbelang zodanig zwaar is dat toestemming niet vereist hoeft te worden. 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 / HR-consulent. Indien de werknemer geen dergelijke markeringen heeft aangebracht, kan de Instelling door inschakeling van een vertrouwenspersoon de betreffende informatie van de werknemer controleren om zo privéinformatie te herkennen en apart te plaatsen alvorens de vervanger of leidinggevende toegang krijgt.

4.6. De inhoud van E-mailberichten wordt niet gecontroleerd. Dit geldt niet voor geautomatiseerde controle (logging en monitoring) op de veiligheid van het e-mailverkeer en netwerk.

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 1.2.

5.3. Verboden tijdens werktijd en / of bij het gebruik van Radboud Universiteit netwerk / Internetverbinding is echter:

- ongewenst gedrag[6];
- 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.

6. Gebruik van sociale media

6.1. Persoonsgegevens of gevoelige gegevens van anderen dienen niet via sociale media gedeeld te worden.

[6] https://www.radboudnet.nl/radboudservices/vm/calamiteiten/ongewenst-gedrag/

6.2. De Instelling accepteert de open dialoog en de uitwisseling van ideeën en het delen van kennis van de werknemer met vakgenoten en derden via sociale media[7].

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.

6.3. 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. Op grond van hun positie moeten zij nagaan of zij op persoonlijke titel kunnen publiceren. Zij moeten zich ervan bewust zijn dat werknemers lezen wat zij schrijven.

6.4. Dit 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.

6.5. 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.

7. Monitoring en controle

7.1. Controle van gebruik van de ICT-faciliteiten en internetgebruik vindt slechts plaats in het kader van veiligheid en handhaving van de regels uit de Gedragscode voor de doelen genoemd bij paragraaf 1.

7.2. Ten behoeve van controle op veiligheid en 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. Bij vermoedens van overtreding van de regels of veiligheid kan in opdracht (van een leidinggevende van een systeembeheerder of CERT-RU) 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 Algemene Verordening Gegevensbescherming 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:

[7] Zie ook: http://www.ru.nl/huisstijl/huisstijltoepassingen/vm-toepassingen/social-media/

- 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. 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.

8. Procedure bij gericht onderzoek

8.1. Gericht onderzoek vindt uitsluitend plaats na schriftelijke opdracht van de decaan / directeur van de betreffende faculteit of het College van Bestuur, waarbij de redenen genoemd worden waarom deze wordt verstrekt. Indien het in opdracht van de directeur / decaan gebeurd, dan ontvangt het College van Bestuur een afschrift van deze opdracht en een vastlegging van de resultaten van het onderzoek.

8.2. 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 de Gedragscode door die werknemer.

8.4. Als gericht onderzoek nader bewijs oplevert, kan de Instelling overgaan tot het kennisnemen van de inhoud van de communicatie of opgeslagen bestanden. De Instelling zal zich maximaal inspannen de identiteit van de personen die deze kennisneming uitvoeren, geheim te houden. De resultaten van het onderzoek worden vastgelegd onder naam van de directeur. Indien het onderzoek geen aanleiding geeft tot verdere maatregelen wordt de vastlegging vernietigd.

8.5. De werknemer wordt zo spoedig mogelijk schriftelijk geïnformeerd door de directeur/decaan of 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. Kort uitstel van het informeren mag alleen als informeren het onderzoek daadwerkelijk zou schaden.

9. Rechten van de werknemer mbt persoonsgegevens

9.1. De werknemer kan zich tot het bestuur[8] wenden met het verzoek om

[8] Via emailadres: mijnprivacy@ru.nl of myprivacy@ru.nl

- het recht op informatie over de verwerkingen;
- het recht op inzage in zijn gegevens;
- het recht op correctie van de gegevens als deze niet kloppen;
- het recht op verwijdering van de gegevens (‘het recht om vergeten te worden’);
- het recht op beperking van de gegevensverwerking;
- het recht om bezwaar te maken tegen de gegevensverwerking;
- het recht op overdracht van zijn gegevens (dataportabiliteit);
- het recht om niet onderworpen te worden aan een geautomatiseerde besluitvorming.

Bij een dergelijk verzoek wordt de medewerker binnen een maand geïnformeerd over de uitvoering van het verzoek.

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

10. Consequenties van overtreding

10.1. Bij handelen in strijd met de Gedragscode 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) worden niet 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 door een beslissing van een bevoegd persoon[9] 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.

11. Slotbepaling

11.1. Deze Gedragscode wordt 1 x per 4 jaar of indien er tussentijds aanleiding voor is, geëvalueerd door het bestuur en andere partijen zoals het medezeggenschapsorgaan.

[9] Bijvoorbeeld CERT-RU of leidinggevende.

11.2. De organisatie kan dit Reglement met instemming van het medezeggenschapsorgaan (de OR) wijzigen als de omstandigheden daar aanleiding toe geven. Voorgenomen wijzigingen worden voorafgaand aan de invoering aan de werknemers bekend gemaakt. Het bestuur zal feedback van werknemers in overweging nemen alvorens de wijzigingen in te voeren.

11.3. In gevallen waarin de Gedragscode niet voorziet, beslist het College van Bestuur.