Radboud Universiteit

Acceptable Use Policy voor studenten

Gedragscode voor ICT- en internetgebruik voor studenten aan 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 model AUP studenten 
2.0	Februari 2018	Commentaar GV verwerkt
2.1	Maart 2018	Commentaar CvB verwerkt
2.2	Mei 2018	Commentaar GV verwerkt

Acceptable Use Policy voor studenten

De Radboud Universiteit (hierna: de Instelling) biedt aan de eigen studenten en aan bezoekende studenten de mogelijkheid internet te gebruiken ten behoeve van de studie. Tevens worden aan studenten voor persoonlijk gebruik een instellingsgebonden mailbox en mogelijkheden tot opslag van bestanden en persoonlijke studiegegevens beschikbaar gesteld ten behoeve van de studie.

Aan het gebruik van deze faciliteiten zijn regels verbonden, in het kader van de goede gang van zaken in de gebouwen en op de terreinen van de Instelling. De regels en eventuele sancties worden beschreven in deze gedragscode, verder te noemen de Gedragscode.

De SR heeft op 2 juli 2018 ingestemd met de inhoud van deze Gedragscode.

1. Gebruik van faciliteiten

Computer- en netwerkfaciliteiten (zoals openbare computers, draadloze en bedrade netwerkaansluitingen, e-mail en internettoegang, opslagcapaciteit, printers en elektronische leeromgevingen) worden aan de student beschikbaar gesteld ten behoeve van de studie, onder meer voor het kunnen maken van opdrachten, verslagen en scripties, het bijhouden van de studievoortgang, het raadplegen van bronnen en het communiceren met docenten en medestudenten.

Het gebruik van eigen apparatuur en toepassingen op de faciliteiten van de Instelling is toegestaan zolang dit gebruik voldoet aan de regels van deze Gedragscode. Het veranderen van instellingen in apparatuur en toepassingen beschikbaar gesteld door de Instelling is alleen toegestaan met aparte toestemming van het systeembeheer[1]. Het aansluiten van eigen netwerkapparatuur waarmee de verbinding kan worden gedeeld met derden op de bedrade of draadloze netwerkaansluitingen is te allen tijde verboden.

Deze 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).

Bepaalde faciliteiten zijn alleen toegankelijk met behulp van een gebruikersnaam en wachtwoord. Deze zijn persoonsgebonden en mogen niet met anderen worden gedeeld. Het systeembeheer kan nadere eisen stellen aan de kwaliteit van wachtwoorden en andere beveiligingsaspecten, zoals nader geformuleerd in het Informatieveiligheidsbeleid. Bij een vermoeden van misbruik van een wachtwoord of authenticatiemiddel kan systeembeheer per direct het betreffende account ontoegankelijk maken.

[1] Dit kan het ISC of een andere erkende RU ondersteuningsgroep zijn.

2. Intellectueel eigendom en vertrouwelijke informatie

De student 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].

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

Het is de student 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[3].

Indien de student in het kader van zijn studie of het uitvoeren van taken voor de Instelling toegang krijgt tot vertrouwelijke informatie of privacy gevoelige informatie waaronder persoonsgegevens, dient de student die informatie strikt vertrouwelijk te behandelen.
De student besteedt bijzondere aandacht aan het treffen van maatregelen zoals in deze Gedragscode genoemd, indien in het kader van het uitvoeren van deze taken 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 en de intellectuele eigendomsrechten voorschriften heeft opgesteld dient de student deze stipt op te volgen.

Radboud Universiteit ’s informatieveiligheid policy en andere informatie over informatie-veiligheid en andere richtlijnen zijn beschikbaar op de RU’s informatieveiligheidspagina’s:

http://www.ru.nl/privacy en www.radboudnet/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 de servicebalie of de ISC-helpdesk.

3. Beveiliging door de Instelling én de student

De Instelling neemt informatieveiligheid serieus. Zij hanteert dan ook een streng beveiligingsbeleid en neemt adequate technische en organisatorische maatregelen om de infrastructuur te beveiligen tegen verlies, diefstal, criminele activiteiten, verlies van

---

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

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

vertrouwelijkheid, schending van privacy-rechten en schending van intellectuele eigendomsrechten.

Natuurlijk is een perfecte beveiliging onmogelijk. Daarom verwacht de Instelling ook van studenten een proactieve houding en serieuze stappen om de eigen computer en andere apparatuur (zoals smartphones of tablets) adequaat te beveiligen. Zo is de student te allen tijde zelf verantwoordelijk voor het gebruik van de eigen apparatuur en de op deze apparatuur opgeslagen gegevens.

In het bijzonder dient de student indien met zijn apparatuur gebruikt wordt gemaakt van de instellingsfaciliteiten in het kader van beveiliging:

- deze apparatuur te voorzien van een adequate virusscanner en firewall;
- regelmatig een reservekopie te maken van alle relevante data, deze kopie, alleen zo lang als die nodig is, veilig op te slaan;
- moeilijk te raden wachtwoorden te gebruiken en deze regelmatig te veranderen;
- deze apparatuur up-to-date te houden wat betreft software-instellingen;
- encryptie toe te passen.

4. Privégebruik en overlast

Beperkt privégebruik van de faciliteiten is toegestaan. 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[4]:

- het in openbare ruimtes raadplegen van internetdiensten met een pornografische, racistische, discriminerende, beledigende of aanstootgevende inhoud of het verzenden van berichten met een dergelijke inhoud[5];
- het verzenden van berichten met een (seksueel) intimiderende inhoud of van berichten die (kunnen) aanzetten tot discriminatie, haat en/of geweld;
- het versturen van berichten aan grote aantallen ontvangers tegelijk, het versturen van kettingbrieven of het verspreiden van kwaadaardige software zoals virussen, wormen, Trojaanse paarden en spyware;

[4] 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. Zie ook https://www.radboudnet.nl/radboudservices/vm/calamiteiten/ongewenst-gedrag/

[5] https://www.radboudnet.nl/publish/pages/852221/17_6_2_protocol_ordemaatregelen_ru_2017_def_zonder_06nr.pdf

- 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 student weet/moet weten 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.

Het gebruik van computer- en netwerkfaciliteiten ten behoeve van commerciële activiteiten is uitsluitend toegestaan wanneer de Instelling hiervoor schriftelijk toestemming heeft verleend.

5. Monitoring door de Instelling

Controle van gebruik van de faciliteiten vindt slechts plaats in het kader van veiligheid en handhaving van de regels uit deze Gedragscode ten behoeve van de goede orde op de Instelling en de bewaking van de integriteit en de veiligheid van het netwerk en de computer-faciliteiten van de Instelling.

Ten behoeve van deze controle op veiligheid en naleving van de regels worden gegevens geautomatiseerd verzameld (gelogd). Deze gegevens zijn toegankelijk voor de direct verantwoordelijke systeembeheerders. Deze kunnen met het oog op het voorkomen van verdere problemen tot technische maatregelen besluiten, zoals een blokkade van de toegang tot een bepaalde dienst of het beperken van de mogelijkheden van het apparaat in kwestie om het netwerk te kunnen gebruiken.

In het bijzonder kan bij overlast, veroorzaakt door apparatuur van studenten, worden overgegaan tot uitschakeling van de netwerktoegangsmogelijkheden. Indien mogelijk wordt de student vooraf gewaarschuwd, zodat hij de gelegenheid heeft de overlast te staken. Wanneer dit vanwege de vereiste spoed niet voorafgaand aan het nemen van de maatregel mogelijk is, doet men zo snel mogelijk melding van de maatregel.

Bij vermoedens van overtreding van de regels of aantasting van veiligheid kan controle worden uitgevoerd op het niveau van individuele verkeersgegevens van het gebruik van de faciliteiten. Slechts bij zwaarwegende redenen vindt controle op de inhoud plaats na opdracht van CERT-RU[6] of leidinggevende van een systeembeheerder.

De Instelling houdt zich bij het controleren op het niveau van verkeersgegevens of de inhoud 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.

[6] Computer Emergency Response Team van de Radboud Universiteit

6. Procedure bij gericht onderzoek

Gericht onderzoek vindt uitsluitend plaats na schriftelijke opdracht van de directeur/ decaan van de 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.

Van gericht onderzoek is sprake wanneer verkeersgegevens of andere persoonsgegevens betreffende de student worden vastgelegd in het kader van een onderzoek naar aanleiding van een zwaarwegend vermoeden van een overtreding van deze Gedragscode door die student.

Als gericht onderzoek nader bewijs oplevert, kan de Instelling overgaan tot het kennisnemen van de inhoud van 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.

De student wordt zo spoedig mogelijk schriftelijk geïnformeerd door de directeur/decaan of door het College van Bestuur over de aanleiding, de uitvoering en het resultaat van het onderzoek. De student 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.

7. Rechten van de student met betrekking tot persoonsgegevens

De student kan zich tot het bestuur[7] wenden met het verzoek om:

- 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 student binnen een maand geïnformeerd over de uitvoering van het verzoek.

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

8. Consequenties van overtreding

Bij handelen in strijd met deze Gedragscode of de algemeen geldende wettelijke regels, kan het bestuur van de Instelling afhankelijk van de aard en de ernst van de overtreding disciplinaire maatregelen treffen. Hieronder vallen een waarschuwing, berisping, een tijdelijke afsluiting of beperking van de faciliteiten (maximaal een jaar) en in extreme gevallen een beëindiging van de inschrijving als student.

Disciplinaire maatregelen (behalve een waarschuwing) worden niet automatisch getroffen op basis van een langs geautomatiseerde weg uitgevoerde verwerking van persoonsgegevens, zoals een constatering van een automatisch filter of blokkade. De student krijgt eerst de gelegenheid zijn zienswijze naar voren te brengen.

In afwijking van het laatste is het mogelijk dat de Instelling bij (geautomatiseerde) constatering van overlast een tijdelijke blokkade van de betreffende faciliteit invoert. Deze blokkade zal maximaal een week worden gehandhaafd of korter als de oorzaak naar tevredenheid van het systeembeheer is weggenomen. Indien na een week geen verbetering is geconstateerd door het systeembeheer, kan het systeembeheer besluiten tot een langere blokkade. Bij herhaling van de oorzaak kunnen disciplinaire maatregelen worden genomen.

9. Slotbepalingen

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. Wijzigingen worden alleen bij het begin van een collegejaar doorgevoerd, behalve in dringende gevallen of wanneer de Instelling door omstandigheden van buitenaf gedwongen is tot een snellere invoering.

Wijzigingen worden alleen ingevoerd nadat de medezeggenschapsraad (de SR) om voorafgaande instemming is gevraagd. Het bestuur zal feedback van studenten in overweging nemen alvorens de wijzigingen door te voeren.

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