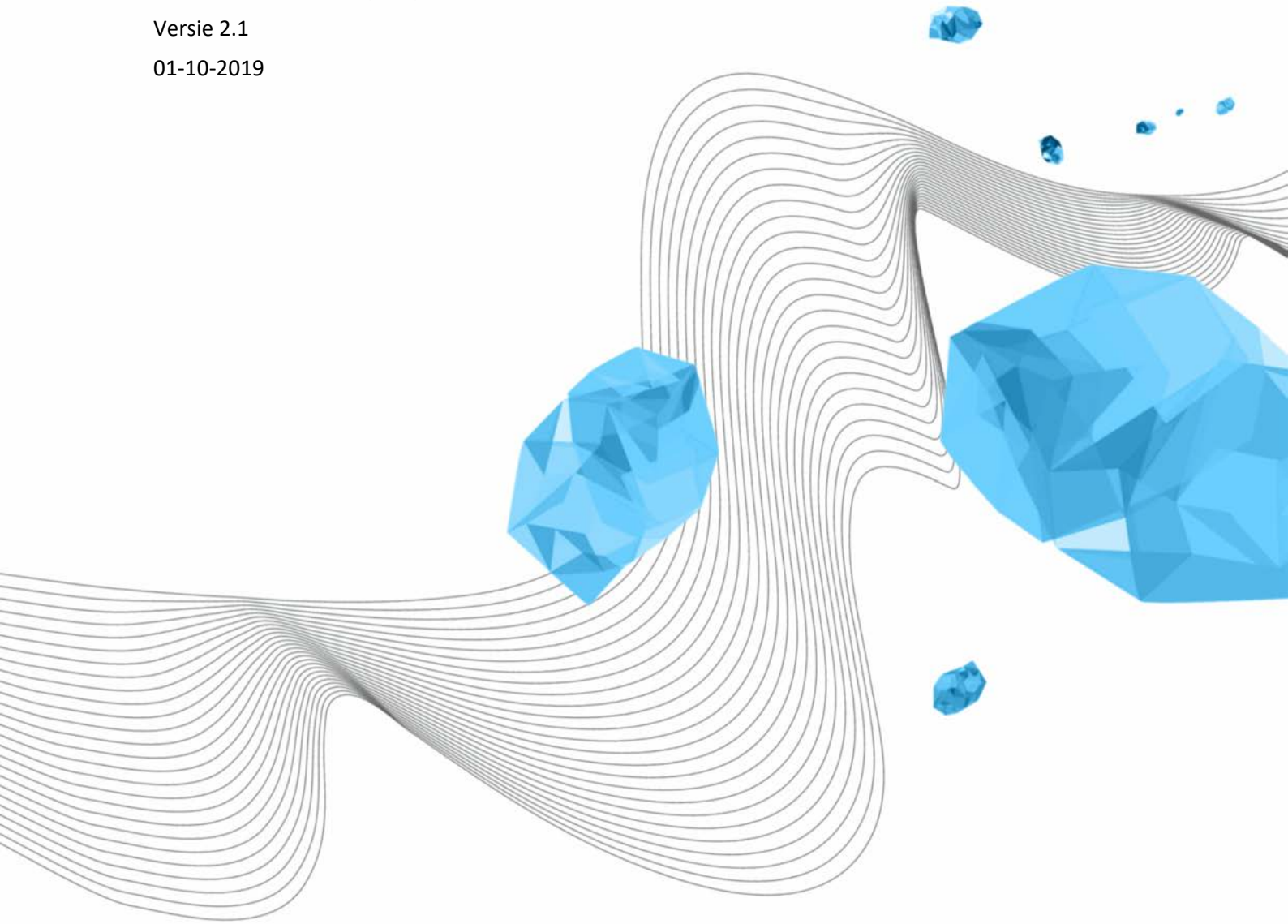
Status: Definitief
Datum vastgesteld in CvB: 11-11-2019
Auteur: Rianne te Brake/Jan Evers

# DIGITALE GEDRAGSCODE VOOR STUDENTEN UNIVERSITEIT TWENTE

Brake - Loeve, A.A. te (LISA)

Versie 2.1

01-10-2019



UNIVERSITY OF TWENTE.

# COLOFON

ORGANISATIE
Library, ICT Services & Archive

TITEL
Digitale gedragscode voor studenten Universiteit Twente

KENMERK
UIM/181205/brk

VERSIE (STATUS)
2.1

DATUM
01-10-2019

AUTEUR(S)
Brake - Loeve, A.A. te (LISA)



# DOCUMENTHISTORIE

| VERSIE | DATUM | AUTEUR(S) | OPMERKINGEN |
|---|---|---|---|
| 1.0 | 2011 | Wim Koolhoven | Definitieve versie |
| 1.4 | 19-11-2018 | Rianne te Brake | Herziene versie:<br>- Structuur volgens actuele SURF model<br>- Actualisatie voor wat betreft stand techniek, privacywetgeving (AVG)<br>- Onderdelen geschrapt die intussen in zelfstandige documenten zijn opgenomen |
| 1.6 | 20-12-2018 | Rianne te Brake | Reacties verwerkt, wijziging sjabloon |
| 1.7 | 15-01-2019 | Jan Evers | Opmerkingen MT LISA verwerkt |
| 1.8 | 06-02-2019 | Jan Evers | Opmerkingen MT LISA en Harma Evers verwerkt |
| 1.9 | 26-02-2019 | Jan Evers | Positief advies UCB (26-02-2019) |
| 2.0 | 15-04-2019 | Jan Evers | 11-03-2019 voorgenomen vaststelling CvB<br>10-04-2019 CvB overleg met UR commissie FPB: ter instemming naar UR en ter informatie naar OPUT<br>15-04-2019 toezeggingen CvB cie FPB aan UR verwerkt |
| 2.1 | 01-10-2019 | Jan Evers | 24-04-2019 UR: instemming onder toevoeging van 1. analyse alleen op basis van UT-account, 2. beheer/ verwerking data op basis van wet- en regelgeving<br>11-11-2019 vastgesteld in CvB |

# DISTRIBUTIELIJST

| VERSIE | DATUM | AUTEUR(S) | GEDISTRIBUEERD AAN |
|---|---|---|---|
| 1.4 | 22-11-2018 | Rianne te Brake | Jan Evers, Henk Swaters, Marc Berenschot, Peter Peters, Erna van der Zandt, Wim Olijslager (security & privacy overleg) |
| 1.6 | 20-12-2018 | Jan Evers | MT LISA |
| 1.7 | 15-01-2019 | Jan Evers | MT LISA, HR – Harma Evers |
| 1.8 | 06-02-2019 | Jan Evers | UCB |
| 1.9 | 27-02-2019 | Jan Evers | CvB |
| 2.0 | 15-04-2019 | Jan Evers | Ter instemming naar UR van 24-04-2019<br>Ter informatie naar OPUT van 27-06-2019 |
| 2.1 | 01-10-2019 | Jan Evers | CvB, ter vaststelling |

# INHOUDSOPGAVE

# 1 BRONVERMELDING

De Digitale gedragscode voor studenten van de Universiteit Twente is gebaseerd op het Model Acceptable Use Policy voor studenten voor het Hoger Onderwijs, een gezamenlijk product van SURFnet en SURFibo. Deze publicatie is beschikbaar onder de licentie Creative Commons Naamsvermelding 3.0 Nederland[1].

# 2 INLEIDING

De Universiteit Twente (hierna: “de Universiteit”) 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 ten behoeve van de studie een mailbox en mogelijkheden tot opslag van bestanden en persoonlijke studiegegevens beschikbaar gesteld. Aan het gebruik van deze faciliteiten zijn regels verbonden. Tegen deze achtergrond mag van studenten verantwoord gebruik van internet en ICT worden verwacht.
Deze gedragscode geldt voor elke student die is ingeschreven bij de Universiteit, onderwijs volgt bij de Universiteit of een studentencampuswoning bewoont en die gebruik maakt van de door de Universiteit geboden ICT-faciliteiten. Daarnaast is deze regeling van toepassing op ex-studenten die vallen onder de Regeling ICT-faciliteiten ex-UT-ers.

# 3 GEBRUIK VAN FACILITEITEN

Computer- en netwerkfaciliteiten (zoals openbare computers, (software-)licenties, draadloze en vaste netwerkaansluitingen, e-mail en internettoegang, opslagcapaciteit, printers en elektronische leeromgeving) 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. Wanneer de Universiteit voor onderwijsdoeleinden specifieke systemen voorschrijft, zal de student alleen deze systemen gebruiken voor de betreffende doeleinden en de daarbij gestelde beperkingen en eisen stipt naleven.

Het gebruik van eigen apparatuur en toepassingen op de faciliteiten van de Universiteit is toegestaan zolang dit gebruik voldoet aan de regels van dit Reglement en de licentievoorwaarden van de leverancier. Het aanbrengen van veranderingen in apparatuur en toepassingen beschikbaar gesteld door de Universiteit is alleen toegestaan met aparte toestemming van systeembeheer. Het aansluiten van eigen netwerkapparatuur waarmee de verbinding kan worden gedeeld met derden op de vaste of draadloze netwerkaansluitingen is te allen tijde verboden, behalve in de woonruimte van studenten.

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

[1] www.creativecommons.org/licenses/by/3.0/nl.

# 4 INTELLECTUEEL EIGENDOM EN VERTROUWELIJKE INFORMATIE

De student maakt geen inbreuk op de intellectuele eigendomsrechten van de Universiteit en derden en respecteert de licentie afspraken zoals die van toepassing zijn binnen de Universiteit.

Indien de student in het kader van zijn studie of het uitvoeren van taken voor de Universiteit toegang krijgt tot vertrouwelijke informatie of privacygevoelige informatie waaronder persoonsgegevens, dient de student die informatie strikt vertrouwelijk te behandelen.
De student besteedt bijzondere aandacht aan het treffen van maatregelen zoals in dit reglement genoemd, indien in het kader van het uitvoeren van deze taken de verwerking van vertrouwelijke informatie buiten de Universiteit noodzakelijk is, zoals via e-mail, in niet Universiteitsgebonden cloud-toepassingen, op externe opslagmedia of eigen client-apparatuur (USB-apparaten, tablets, etc.).

Indien de Universiteit met betrekking tot het waarborgen van de vertrouwelijkheid en de intellectuele eigendomsrechten voorschriften heeft opgesteld dient de student deze stipt op te volgen.

# 5 BEVEILIGING DOOR DE UNIVERSITEIT ÉN DE STUDENT

De Universiteit neemt informatiebeveiliging 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 vertrouwelijkheid, schending van privacy-rechten en schending van intellectuele eigendomsrechten. Perfecte beveiliging is onmogelijk. Daarom verwacht de Universiteit ook van studenten een proactieve houding om de eigen computer en andere apparatuur (zoals smartphones of tablets) adequaat te beveiligen. De student is te allen tijde zelf verantwoordelijk voor het gebruik van de eigen apparatuur en de op deze apparatuur opgeslagen gegevens. De student treft beveiligingsmaatregelen conform de adviezen en aanwijzingen van het cybersafety-team van de Universiteit[2]. Het cybersafety team heeft geen formele status en bevoegdheden. Het team bevordert awareness op het gebied van cybersafety. De leden zijn medewerkers van HR, M&C, LISA. Het team geeft adviezen en aanwijzingen op basis van vastgesteld beleid.

# 6 PRIVÉGEBRUIK EN OVERLAST

Beperkt privégebruik van de ICT- en internetfaciliteiten is toegestaan. Gebruik, privé of ten behoeve van studie, mag niet storend zijn voor de goede orde bij de Universiteit en mag geen overlast veroorzaken bij anderen, mag geen inbreuk maken op rechten van de Universiteit of derden of de integriteit en de veiligheid van het netwerk aantasten. Daarnaast geldt dat privégebruik alleen is toegestaan wanneer de licentievoorwaarden van de leverancier dit toelaten. De Universiteit is niet verplicht reservekopieën te maken van opgeslagen privébestanden of –informatie op systemen van de Universiteit of hiermee rekening te houden bij vervanging of reparatie van betreffende systemen. Als verboden, storend en/of overlast veroorzakend gebruik geldt:

[2] Bijvoorbeeld het Cybersafety 10-stappenplan.

- 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;
- 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.

Studenten die in hun privé woonruimte met privé middelen gebruik maken van een netwerkfaciliteit van de Universiteit kunnen geen beperkingen opgelegd worden aan het gebruik, behoudens voor zover noodzakelijk om de integriteit en de veiligheid van het netwerk te kunnen bewaren, of om de gevolgen van overbelasting te beperken. Indien de Universiteit ingrijpt om de gevolgen van overbelasting te beperken, zullen gelijke soorten verkeer gelijk worden behandeld. De overige bepalingen in dit reglement zijn onverkort van toepassing voor studenten die in hun woonruimte gebruik maken van een netwerkfaciliteit van de Universiteit.
Het gebruik van computer- en netwerkfaciliteiten ten behoeve van commerciële activiteiten is uitsluitend toegestaan wanneer de Universiteit hiervoor schriftelijk toestemming heeft verleend.

# 7 MONITORING DOOR DE UNIVERSITEIT

Controle van gebruik van de faciliteiten vindt slechts plaats in het kader van handhaving van de regels uit deze gedragscode. Ten behoeve van deze controle worden geautomatiseerd gegevens verzameld (gelogd). De data van studenten wordt uitsluitend verzameld en geanalyseerd op basis van een geregistreerd account van de student op de ICT-systemen van de Universiteit. Bij beheer en verwerking van deze data wordt de nationale wet- en regelgeving aangehouden. Deze gegevens zijn alleen toegankelijk voor de verwerkingsverantwoordelijke of medewerkers met een toezichthoudende en/of uitvoerende taak in het kader van een gericht onderzoek. Deze gegevens worden alleen in geanonimiseerde vorm aan overige medewerkers beschikbaar gesteld, tenzij dit onmogelijk is voor het uitvoeren van beheertaken.
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 wegens de vereiste spoed niet voorafgaand aan het nemen van de maatregel mogelijk is, doet men zo snel mogelijk daarna melding van de maatregel.
Bij vermoedens van overtreding van de regels uit deze gedragscode kan het CvB opdracht geven tot het uitvoeren van een gericht onderzoek (zie paragraaf 8). Op basis van een gericht onderzoek mag e-mail van een student gecontroleerd worden zonder toestemming te vragen aan de betreffende student. Niet alle bij wet verboden activiteiten staan expliciet in deze gedragscode vermeld. Op deze bij wet verboden activiteiten kan echter wel gecontroleerd worden. Een voorbeeld hiervan is het downloaden van illegaal materiaal.
De Universiteit houdt zich bij het uitvoeren van een gericht onderzoek onverkort aan de Algemene Verordening Gegevensbescherming en andere relevante wet- en regelgeving. In het bijzonder beveiligt de Universiteit de bij controle vastgelegde gegevens tegen ongeautoriseerde toegang.
E-mailberichten van Universiteitsraadleden, faculteitsraadleden en leden van de opleidingscommissies in functie worden niet gecontroleerd voor zover deze betrekking hebben op hun functie als lid van de medezeggenschap/opleidingscommissie. Dit geldt niet voor geautomatiseerde controle op de veiligheid van het e-mailverkeer en netwerk.

# 8 GERICHT ONDERZOEK

Bij zwaarwegende vermoedens van overtreding van deze, of andere, gedragscode door een student heeft de UT het recht om een gericht onderzoek uit te voeren. Voor het uitvoeren van een gericht onderzoek is altijd een opdracht vanuit het CvB nodig. De UT garandeert dat een gericht onderzoek op een zorgvuldige manier wordt uitgevoerd.

# 9 CONSEQUENTIES VAN OVERTREDING

Bij handelen in strijd met dit Reglement of de algemeen geldende wettelijke regels, kan het College van Bestuur van de Universiteit afhankelijk van de aard en de ernst van de overtreding maatregelen treffen.
Hieronder vallen een waarschuwing, een tijdelijke afsluiting of beperking van de faciliteiten (maximaal een jaar) en in extreme gevallen een beëindiging van de inschrijving als student.
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. Hiervoor is altijd menselijke beoordeling nodig. Voorts worden geen maatregelen getroffen zonder dat de student gelegenheid heeft gekregen zijn zienswijze naar voren te brengen.
In afwijking van het voorgaande is het mogelijk dat de Universiteit bij (geautomatiseerde) constatering van overlast of een beveiligingsrisico 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 maatregelen worden genomen.

# 10 SLOTBEPALINGEN

Deze gedragscode wordt tweejaarlijks geëvalueerd. Wijzigingen worden alleen ingevoerd nadat de Universiteitsraad heeft ingestemd. Het College van Bestuur kan feedback van studenten in overweging nemen alvorens de wijzigingen in te voeren.
In gevallen waarin deze gedragscode niet voorziet, beslist het College van Bestuur.
Deze gedragscode vervangt de Gedragscode ICT- en internetgebruik Universiteit Twente studenten 2011.