Gedragscode ICT- en Internetgebruik

Universiteit Twente

2009

INHOUDSOPGAVE

Woord vooraf

Deze Gedragscode geeft de wijze aan waarop bij de Universiteit Twente wordt omgegaan met ICT- en Internetgebruik. De code regelt het verantwoord gebruik van ICT-voorzieningen en Internet en de wijze waarop controle op het gebruik plaatsvindt. Het streven is een goede balans aan te brengen tussen verantwoord en veilig ICT- en Internetgebruik en de privacy van de gebruiker.

Omdat voor studenten een eigen Gedragscode voor ICT- en Internetgebruik zal worden opgesteld, is deze code niet van toepassing op de student die gebruik maakt van de ICT- en Internetvoorzieningen van de Universiteit Twente.

Bij het opstellen van deze gedragscode is aansluiting gezocht bij de Wet bescherming persoonsgegeven (WBP). Deze wet is van toepassing als er sprake is van verwerking van persoonsgegevens. Verwerking betreft het gehele proces van verzamelen tot aan vernietigen van gegevens. Gegevens met betrekking tot het e-mail en internetgebruik zijn in het algemeen te kwalificeren als persoonsgegevens omdat deze gegevens herleidbaar zijn tot natuurlijke personen.

1. Definities

In deze regeling wordt verstaan onder:

a. **Beheerder**: de natuurlijke persoon die belast is met beheer van de faculteit (decaan), het onderzoeksinstituut (wetenschappelijk directeur) dan wel een dienst (directeur).

b. **CERT-UT**: het Computer Emergency Response Team van de Universiteit Twente, ingesteld om in opdracht van het College van Bestuur onder verantwoordelijkheid van de directeur ICTS computerveiligheidsproblemen binnen de Universiteit Twente aan te pakken en waar mogelijk te voorkomen.

c. **College van Bestuur**: College van Bestuur Universiteit Twente.

d. **Directeur ICTS**: de directeur van het ICT-Servicecentrum van de Universiteit Twente.

e. **Gebruiker**: een ieder – met uitzondering van de student zoals onder k. genoemd – die gebruik maakt van de ICT-voorzieningen die de Universiteit Twente ter beschikking stelt, waaronder een ieder die zich met een ICT-werkplek op het Internet manifesteert met een identiteit van de Universiteit Twente (IP-nummer van de Universiteit Twente of een domeinnaam onder het hoofddomein UTWENTE.NL).

f. **Gedragscode**: de hier vastgelegde Gedragscode ICT- en Internetgebruik.

g. **ICT- en Internetgebruik**: ieder gebruik via het UTnet, SURFnet of Internet van door de Universiteit Twente geboden ICT-faciliteiten, inclusief e-mailvoorziening.

h. **ICT-functionaris**: elke werknemer van de Universiteit Twente met een functie die behoort bij het ICT-Servicecentrum, de directeur ICTS, alsmede andere personen die onder de verantwoordelijkheid van de Universiteit Twente werkzaamheden verrichten op ICT-gebied.

i. **ICT-werkplek**: een computer (PC, Laptop, PDA, e.d.) die de gebruiker hanteert voor het ICT- en Internetgebruik.

j. **Persoonsgegevens**: alle gegevens die informatie kunnen verschaffen over een identificeerbare natuurlijke persoon.

k. **Student**: een ieder die als student staat ingeschreven bij de Universiteit Twente dan wel onderwijs volgt bij de Universiteit Twente.

l. **SURFnet:** de landelijke netwerkinfrastructuur die onder beheer is van SURFnet BV, waarmee de locale netwerken van de instellingen van hoger onderwijs en onderzoek onderling verbonden zijn en waarop het UTnet is aangesloten.

m. **SURFnet BV:** de BV onder Stichting SURF die het SURFnet beheert.

n. **Toegangsconfiguratie**: instellingen van ICT-werkplekken, servers en netwerkapparatuur ten behoeve van identificatie van het systeem op en netwerkverkeer over het netwerk.

o. **Toegangssleutel**: een combinatie van gebruikersnaam en wachtwoord of andere authenticatiefaciliteit die de gebruiker autoriseert tot gebruik van ICT-voorzieningen van de Universiteit Twente.

p. **Universiteit**: Universiteit Twente.

q. **UTnet**: het intranet van de Universiteit Twente, zowel bedraad als draadloos, dat alle computersystemen binnen de Universiteit met elkaar verbindt, inclusief rechtstreeks aangesloten thuiswerkplekken, en dat gekoppeld is aan SURFnet en Internet.

r. **Verkeersgegevens**: gegevens over netwerk-, toegangs- en computergebruik zoals accountnaam, bron, afzender, geadresseerde, bestemming, datum, tijd en omvang.

s. **Wbp**: Wet bescherming persoonsgegevens.

t. **Werknemer**: een ieder die een dienstverband heeft met de Universiteit Twente dan wel een ieder die op een andere basis is tewerkgesteld bij de Universiteit Twente.

2. Reikwijdte

2.1. Deze Gedragscode is van toepassing op een ieder – met uitzondering van de student zoals onder k. bij definities genoemd - die gebruik maakt van de door de Universiteit geboden ICT-faciliteiten, inclusief e-mailvoorziening.

3. ICT- en Internetgebruik algemeen

3.1. Het doel van deze Gedragscode is om voor gebruikers duidelijkheid te verschaffen over het kader waarbinnen ICT- en Internetgebruik bij de Universiteit dient plaats te vinden en welke maatregelen genomen kunnen worden bij handelen dat in strijd met deze Gedragscode is.

3.2. De gebruiker onthoudt zich bij het ICT- en Internetgebruik van handelingen die de goede naam van de Universiteit schade kunnen toebrengen, onrechtmatig of strafbaar zijn.

3.3. De door de Universiteit aan de gebruiker verleende toegangssleutel is strikt persoonlijk en blijft eigendom van de Universiteit. Het is niet toegestaan de toegangssleutel aan derden te verstrekken, tenzij dit noodzakelijk is voor een adequate uitoefening van de werkzaamheden en dan alleen na toestemming van de beheerder. Degene aan wie de toegangssleutel is verstrekt, is verplicht al hetgeen te doen dan wel na te laten wat redelijkerwijs van hem/haar mag worden verwacht om misbruik van de verstrekte toegangssleutel te voorkomen.

3.4. Een gebruiker kan zelf een derde technisch een machtiging verlenen om toegang tot zijn e-mailvoorziening (inclusief agenda) te krijgen. De derde gebruikt hiervoor zijn eigen toegangssleutel.

3.5. Bij gebleken of vermoede beveiligingsincidenten dient de gebruiker het incident onverwijld te melden bij het CERT-UT.

3.6. Het is de gebruiker verboden de toegangsconfiguratie van ICT-werkplekken, servers en netwerkapparatuur van de Universiteit te wijzigen.

3.7. Het is de gebruiker zonder voorafgaande toestemming van directeur ICTS niet toegestaan om niet-publieke informatie of diensten op het UTnet op enigerlei wijze te ontsluiten voor de buitenwereld.

3.8. Het is de gebruiker niet toegestaan om andere netwerkapparatuur (zoals routers en switches) op het UTnet aan te sluiten dan waarvoor de directeur ICTS toestemming heeft gegeven.

3.9. De gebruiker mag bij het ICT- en Internetgebruik de ICT-infrastructuur van de Universiteit niet verstoren of onevenredig belasten.

Het is de gebruiker in ieder geval niet toegestaan om 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.

3.10. Het is de gebruiker in ieder geval niet toegestaan bewust internetsites te bezoeken die (kinder-) pornografisch, racistisch of anderszins discriminerend materiaal bevatten, tenzij dit noodzakelijk is ten behoeve van de vrije informatievergaring in het kader van de functie-uitoefening en hiervoor toestemming bij de beheerder is verkregen.

3.11. Het is de gebruiker in ieder geval niet toegestaan dreigende, (seksueel) intimiderende, (kinder)pornografische dan wel racistische of anderszins discriminerende e-mailberichten te versturen of op te slaan.

3.12. E-mailberichten van en naar de Universiteit worden onder verantwoordelijkheid van de directeur ICTS gecontroleerd op malware (virussen, en dergelijke) en spam. Zonodig worden besmette berichten verwijderd of ontdaan van malware.

3.13 De gebruiker dient bij gebruik van de e-mailvoorziening van de Universiteit als afzender een e-mailadres te gebruiken dat door de Universiteit aan de gebruiker is verstrekt. Het is de gebruiker niet toegestaan het e-mailadres als afzendadres ter beschikking te stellen aan anderen.

3.14. Het is de gebruiker niet toegestaan om voor anderen bestemde e-mailberichten te lezen, kopiëren, wijzigen of wissen, tenzij daarvoor expliciet door de geadresseerde toestemming is verleend of het plaatsvindt in het kader van het gerichte onderzoek zoals onder artikel 8 genoemd.

4. Back-ups

4.1. De gebruiker mag er zonder tegenbericht van ICTS van uitgaan, dat de back-up procedures bij de Universiteit blijvend betrouwbare back-ups leveren. Mocht de gebruiker voor dataopslag media gebruiken die niet standaard wordt gebackupt, dan dient hij hier zelf voor zorg te dragen. Zonodig in samenspraak met ICTS.

5. ICT- en Internetgebruik door werknemers

5.1. De werknemer dient het ICT- en Internetgebruik in te zetten ten behoeve van de functie-uitoefening.

5.2. Het is de werknemer toegestaan het ICT- en Internetgebruik in beperkte mate in te zetten voor privédoeleinden, mits dit niet storend is voor de dagelijkse werkzaamheden van de werknemer of van anderen en anderen er geen aanstoot aan kunnen nemen.

5.3. Het ICT- en Internetgebruik door de werknemer ten behoeve van nevenwerkzaamheden is uitsluitend toegestaan als en voor zover de beheerder hiervoor schriftelijk toestemming heeft verleend.

5.4. Verder zijn de overige bepalingen in deze Gedragscode onverkort voor werknemers van toepassing.

6. Algemeen toezicht

6.1. Algemeen toezicht heeft systeem- en netwerkbeveiliging ten doel en vindt plaats door een ICT-functionaris in opdracht van de directeur ICTS.

6.2. Door CERT-UT kunnen verkeersgegevens bij een beveiligingsincident worden onderzocht met uitsluitend als doel de oorzaak van het incident te vinden en weg te nemen of de gevolgschade van het incident te beperken. In dat kader kan CERT-UT tijdelijke beperkingen aan de gebruiker opleggen in de toegang tot bepaalde ICT-faciliteiten. De gebruiker dient aan dit onderzoek mee te werken door relevante gegevens ter beschikking te stellen en de aanwijzingen van CERT-UT op te volgen.

6.3. Verkeersgegevens over ICT- en Internetgebruik worden in beginsel niet langer bewaard dan zes maanden. Ingeval van een gericht onderzoek als bedoeld in artikel 8 kunnen deze gegevens langer worden bewaard, totdat de noodzaak daartoe is vervallen.

6.4. De ICT-functionaris heeft geheimhoudingsplicht met betrekking tot gegevens over ICT- en internetgebruik die tot personen herleidbaar zijn.

7. Gericht onderzoek

7.1. Bij een vermoeden van gebruik in strijd met de Gedragscode wordt de betreffende gebruiker zo spoedig mogelijk op zijn/haar gedrag aangesproken door de beheerder.

7.2. Gericht onderzoek naar een persoon vindt plaats naar aanleiding van gerechtvaardigde vermoedens dan wel constatering van onjuist gebruik als bedoeld in de artikelen 3, 5 en 6 van deze Gedragscode. Gericht onderzoek heeft als hoofddoelen:

- het vaststellen van oneigenlijk ICT- en Internetgebruik;
- het controleren van gemaakte afspraken over het (verboden) gebruik;
- het controleren of bedrijfsgeheimen voldoende worden beschermd en niet openbaar worden of zijn gemaakt;
- het voorkomen van negatieve publiciteit over de Universiteit.

7.3. Het gerichte onderzoek vindt plaats na schriftelijke opdracht van het College van Bestuur aan de directeur ICTS en wordt uitgevoerd door een daartoe aangewezen ICT-functionaris. In de opdracht van het College van Bestuur wordt vermeld waarom het onderzoek plaatsvindt en waarom – voor zover dit aan de orde is – de gebruiker pas achteraf van het onderzoek op de hoogte wordt gesteld.

7.4. Het College van Bestuur wordt schriftelijke geïnformeerd over de resultaten van het onderzoek. Indien het onderzoek geen aanleiding geeft tot verdere maatregelen wordt het schriftelijke verslag vernietigd.

7.5. Alleen bij zwaarwegende redenen vindt gericht onderzoek naar inhoud van e-mails en opgeslagen bestanden plaats. In de schriftelijke opdracht van het College van Bestuur worden deze redenen genoemd.

7.6. E-mailberichten en bestanden van Universiteitsraad- en OPUT-leden in functie, leden van Faculteits- en Dienstraden in functie, bedrijfsartsen en andere werknemers[1] met een door het College van Bestuur verleende vertrouwensfunctie zijn in beginsel uitgesloten van gericht onderzoek. Dit geldt niet voor het algemene toezicht op de systeem- en netwerkbeveiliging.

7.7. De gebruiker ten wiens laste een onderzoek als bedoeld in artikel 7.3. plaatsvindt, wordt zo spoedig mogelijk door het College van Bestuur schriftelijk geïnformeerd over de aanleiding, uitvoering en het resultaat van het onderzoek. De gebruiker wordt in de gelegenheid gesteld uitleg te geven over de aangetroffen gegevens. Het verstrekken van informatie aan de gebruiker wordt uitgesteld indien het onderzoek daardoor wordt geschaad.

7.8 Zaken die niet op ICT-werkplekken en computersystemen van de Universiteit thuishoren zoals illegale software, films en muziek, worden in opdracht van de beheerder verwijderd. De gebruiker wordt hierover vooraf geïnformeerd tenzij het onderzoek daardoor wordt belemmerd.

8. Sancties

8.1. Als de gebruiker in strijd met de Gedragscode handelt, kan het College van Bestuur de volgende sancties opleggen:

a. al dan niet tijdelijke beperking in de toegang tot bepaalde ICT-faciliteiten;
b. tijdelijk of definitief verbod tot het gebruik van bepaalde ICT-faciliteiten;
c. betalen van kosten voortvloeiend uit het geconstateerde misbruik;
d. overige (rechtspositionele) maatregelen waaronder maatregelen zoals genoemd in de Regeling Disciplinaire maatregelen Universiteit Twente.

9. Aansprakelijkheid

9.1. De Universiteit behoudt zich het recht voor de gebruiker aansprakelijk te stellen voor schade die de gebruiker teweeg brengt als gevolg van ICT- en Internetgebruik door de gebruiker. Hieronder valt tevens de schadevergoeding die een derde bij de Universiteit claimt ten gevolge van in strijd met de Gedragscode door de gebruiker verrichte handelingen.

9.2. De Universiteit sluit aansprakelijkheid uit voor elke schade die voortvloeit uit het gebruik en het niet (volledig) kunnen gebruiken van de ICT-voorzieningen van de Universiteit.

10. Slotbepalingen

10.1. Twee jaar na invoering van deze Gedragscode zal deze worden geëvalueerd.

10.2. De Wpb is onverkort van toepassing.

[1] Het College van Bestuur stelt een lijst op met medewerkers die worden geacht een vertrouwensfunctie te vervullen

10.3. Deze Gedragscode is met terugwerkende kracht vanaf 1 januari 2010 op 8 maart 2010 door het College van Bestuur en met instemming van de Universiteitsraad (op 4 november 2009) vastgesteld.