



Vrije Universiteit
Personeelsbalie Servicecentrum
De Boelelaan 1105
1081 HV Amsterdam

telefoon (020) 59 85400
fax (020) 59 85454
e-mail personeelsbalie@dienst.vu.nl
internet www.intranet.vu.nl/personeelsbalie >
Regelingen personeel

Gedragcode computer- en netwerkgebruik

05/2009

Woord vooraf

1. Definities
2. Algemene uitgangspunten
3. Computer- en netwerkgebruik
4. Algemeen toezicht en gericht onderzoek
5. Maatregelen
6. Bezwaar
7. Slotbepalingen

Woord vooraf

De Vrije Universiteit stelt computers en haar netwerk ter beschikking aan onder andere studenten en werknemers om toegang te krijgen tot ondermeer e-mail en internet. Uitgangspunt hierbij is dat de gebruikers van het VU-netwerk hiermee op een verantwoorde en adequate manier omgaan.

Zoals reeds in het Statuut VU is omschreven, behoren de leden van de universitaire gemeenschap zich te onthouden van gedragingen die inbreuk maken op het normale functioneren van de universiteit, opzettelijk schade toebrengen aan de werkzaamheden aan de universiteit of in strijd zijn met de gangbare opvattingen van fatsoen en behoorlijk gedrag in het onderlinge verkeer, een en ander mede gezien in het licht van de doelstelling van de Vrije Universiteit. Deze gedragscode is ook op te vatten als een verbijzondering van artikel 1.8 lid 2 en 3 CAO en artikel 1.3 lid 3 Statuut VU.

Deze gedragscode is opgesteld om de gebruikers van het VU-computers en van het VU-netwerk (hierna: netwerk) bekend te maken met hetgeen de Vrije Universiteit verantwoord en adequaat acht ten aanzien van gebruik ervan. Hierbij moet in ieder geval worden gedacht aan beperkt privégebruik, het voorkomen van overbelasting van het netwerk, zich onthouden van computer- en netwerkgebruik dat godslasterlijk, pornografisch, intimiderend of anderszins discriminerend is.

De gebruikers van het VU-netwerk dienen zich aan deze gedragscode te houden. Ook beoogt deze gedragscode tegen te gaan dat de gebruikers hinder ondervinden van ongewenst gebruik van het VU-netwerk. De Vrije Universiteit streeft naar een goede balans tussen gericht onderzoek naar onverantwoord gebruik en de privacybescherming van de gebruikers.

Deze gedragscode stelt regels ten aanzien van computer- en netwerkgebruik, en geeft voorschriften over de wijze waarop toezicht op en onderzoek naar de naleving ervan plaatsvinden.

Algemeen toezicht heeft ten doel systeem- en netwerkbeveiliging.

Gericht onderzoek naar persoonsgegevens van de gebruiker in het kader van deze code heeft als hoofddoelen:

- tegengaan van oneigenlijk en bovenmatig gebruik van e-mail en internet, datanetwerk en opslagcapaciteit;
- naleving afspraken over verboden gebruik;
- beveiligen bedrijfssystemen en -netwerk.

1. Definities

Gebruiker: eenieder die gebruik maakt van het VU-netwerk.

Werknemer: eenieder die valt onder het begrip werknemer zoals omschreven in artikel 1.1 sub i van de CAO alsmede de gastvrijheidgenieter en degene die op andere basis werkzaamheden voor de Vrije Universiteit verricht.

Student: degene die als zodanig is ingeschreven bij de Vrije Universiteit alsmede de extraneus en degene die anderszins een opleiding of cursus aan de Vrije Universiteit volgt.

2. Algemene uitgangspunten

- 2.1 De gedragscode is van toepassing op al het gebruik van, door de Vrije Universiteit beschikbaar gestelde, computers en netwerken, waaronder e-mail- en internetgebruik. Deze gedragscode beoogt de gangbare normen die van toepassing zijn op voornoemd gebruik te formuleren.
- 2.2 De door de Vrije Universiteit aan gebruikers verleende accounts zijn strikt persoonlijk. Het is dan ook niet toegestaan informatie over gebruikersnaam of wachtwoord/toegangscodes aan derden te verstrekken. Degene aan wie de accounts zijn verstrekt, is verplicht al hetgeen te doen dan wel na te laten wat redelijkerwijs van hem mag worden verwacht om misbruik van de verstrekte accounts te voorkomen.

3. Computer- en netwerkgebruik

- 3.1 De door de Vrije Universiteit beschikbaar gestelde computer en netwerk dienen te worden gebruikt ten behoeve van de functie-uitoefening respectievelijk studie.
- 3.2 Het is werknemers daarnaast toegestaan in beperkte mate de computer en het netwerk, waaronder e-mail en internet, voor privédoeleinden te gebruiken mits dit niet storend is voor de dagelijkse werkzaamheden van hen of van anderen en anderen er geen aanstoot aan kunnen nemen.
- 3.3 Het is in ieder geval niet toegestaan godslasterlijke, dreigende, (seksueel) intimiderende, (kinder-) pornografische dan wel racistische of anderszins discriminerende e-mailberichten te versturen.
- 3.4 Het is in ieder geval niet toegestaan bewust internetsites te bezoeken die godslasterlijk, (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. Het is tevens niet toegestaan om op de door de Vrije Universiteit verschaft (persoonlijke) internetpagina links aan te brengen naar internetpagina's met voornoemde inhoud of materiaal van genoemde aard op het VU-domein (-en), tenzij dit noodzakelijk is voor de vrije informatievergaring in het kader van de functie-uitoefening.
- 3.5 Opslag en verwerking van onrechtmatig verkregen informatie of informatie waarvan het bezit strafbaar is, zijn niet toegestaan, ook niet voor privédoeleinden.
- 3.6 Het privégebruik van het netwerk, waaronder e-mail en internetgebruik en de opslag van privébestanden, mag geen onevenredige belasting vormen voor de IT-infrastructuur van de Vrije Universiteit.

4. Algemeen toezicht en gericht onderzoek

- 4.1 Algemeen toezicht door een daartoe aangewezen IT-functionaris heeft ten doel systeem- en netwerkbeveiliging. Algemeen toezicht houdt in het zorgdragen dat onbevoegden geen toegang krijgen tot (persoons)gegevens, systemen en netwerken en daarnaast dat bevoegden continu en veilig gebruik kunnen maken van het netwerk.
- 4.2 Beheerders IT hebben geheimhoudingsplicht met betrekking tot netwerkgegevens, waaronder gegevens van e-mail- en internetgebruik, die tot personen herleidbaar zijn. Beheerders IT nemen zodanige maatregelen dat een passend beveiligingsniveau wordt bereikt gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen.
- 4.3 Verkeersgegevens (gegevens over afzender, bestemming, datum, tijd, hoeveelheid en omvang) over e-mail- en internetgebruik worden in beginsel niet langer bewaard dan zes maanden. Ingeval van een vermoeden van onjuist gebruik kunnen deze gegevens langer worden bewaard totdat de noodzaak daartoe is vervallen, hetgeen conform de Wet bescherming persoonsgegevens wordt gemeld bij het College Bescherming Persoonsgegevens.
- 4.4 Bij een vermoeden van onjuist gebruik als bedoeld in de artikelen 3.2 t/m 3.6 wordt de desbetreffende werknemer respectievelijk student zo spoedig mogelijk door de directeur respectievelijk decaan op zijn gedrag aangesproken. De werknemer respectievelijk student wordt in de gelegenheid gesteld uitleg te geven.

- 4.5 Gericht onderzoek vindt slechts plaats naar aanleiding van gerechtvaardigde vermoedens dan wel constatering van onjuist gebruik zoals bedoeld in de artikelen 3.2 t/m 3.6. Het onderzoek beperkt zich in principe tot verkeersgegevens van het gebruik van e-mail en internet en in het kader van de netwerkveiligheid tot de geautoriseerde. Het onderzoek dat een student betreft, vindt plaats na schriftelijke opdracht van de decaan van de desbetreffende faculteit. Het onderzoek dat een werknemer betreft, vindt plaats na schriftelijke opdracht van de decaan respectievelijk directeur. Het College van Bestuur ontvangt een afschrift van deze opdracht en een schriftelijk verslag van de resultaten van het onderzoek.
- 4.6 Indien het onderzoek geen aanleiding geeft tot verdere maatregelen wordt het schriftelijk verslag vernietigd.
- 4.7 E-mailberichten van OR- en USR-leden in functie, bedrijfsartsen en andere werknemers met een vertrouwensfunctie zijn in beginsel uitgesloten van gericht onderzoek. Dit geldt niet voor het algemene toezicht op de systeem- en netwerkveiligheid.
- 4.8 Alleen bij zwaarwegende redenen vindt na schriftelijke toestemming van het College van Bestuur gericht onderzoek naar de inhoud van bestanden, waaronder e-mail, plaats. In de schriftelijke toestemming worden deze redenen genoemd.
- 4.9 De werknemer respectievelijk student ten wiens laste een onderzoek als bedoeld in artikel 4.5 of 4.8 plaatsvindt, wordt zo spoedig mogelijk schriftelijk geïnformeerd door de directeur respectievelijk decaan over de aanleiding, de uitvoering en het resultaat van het onderzoek. De werknemer of student wordt in de gelegenheid gesteld uitleg te geven over de aangetroffen gegevens. Het verstrekken van informatie aan de werknemer wordt uitgesteld indien het onderzoek daardoor wordt geschaad.
- 4.10 Zaken die niet in VU-systemen, netwerken en -PC's thuishoren zoals illegale of te zeer netwerkbelastende software, films en muziek, worden in opdracht van de betrokken decaan respectievelijk directeur verwijderd. De werknemer of student wordt hierover vooraf geïnformeerd, tenzij het onderzoek daardoor wordt belemmerd.

5. Maatregelen

- 5.1 Wanneer uit gericht onderzoek blijkt dat sprake is van onjuist gebruik van het door de Vrije Universiteit beschikbaar gestelde computer- en of netwerk, worden studenten en gebruikers daarop aangesproken door de decaan respectievelijk directeur en worden eventueel passende maatregelen genomen.
- 5.2 In geval van onjuist gebruik door een werknemer kan het College van Bestuur passende maatregelen, waaronder ontslag op staande voet als meest vergaande maatregel, worden genomen respectievelijk sancties opleggen.
- 5.3 In geval van onjuist gebruik door een student kan het College van Bestuur passende maatregelen, waaronder het aan de student ontzeggen van de toegang tot de faciliteiten, gebouwen en terreinen van de Vrije Universiteit voor maximaal een jaar als meest vergaande maatregel, nemen.

6. Bezwaar

- 6.1 De werknemer respectievelijk student ten aanzien van wie gericht onderzoek als bedoeld in artikel 4.5 of 4.8 is of wordt uitgevoerd kan daartegen schriftelijk en gemotiveerd bezwaar aantekenen bij het College van Bestuur binnen vier weken nadat de werknemer is ingelicht over het onderzoek.
- 6.2 Het College van Bestuur geeft een schriftelijke en met redenen omklede reactie binnen vier weken na ontvangst van het bezwaar. Indien het bezwaar als bedoeld in het vorige lid gegrond wordt verklaard, worden de door middel van de onderzoeksmaatregelen verkregen gegevens terstond vernietigd. Tevens worden eventuele maatregelen ingetrokken indien deze - naar achteraf blijkt uit het nader onderzoek - ten onrechte zijn genomen.

7. Slotbepalingen

- 7.1 Deze gedragscode is tot stand gekomen met instemming van de Ondernemingsraad en na advies van de Universitaire Studentenraad.
- 7.2 De Wet bescherming persoonsgegevens is onverkort van toepassing.
- 7.3 In gevallen waarin de regeling niet voorziet, beslist het College van Bestuur.