Gedragscode internet en e-mailgebruik

Het bestuur van CSG Het Noordik
Gelet op
- Artikel 7:660 van het Burgerlijk Wetboek
- De Wet Bescherming Persoonsgegevens
- Artikel 27 lid 1 sub k en l Wet op de ondernemingsraden

Overwegende dat

- Het gebruik van internet en e-mail voor de werknemers (inclusief gedetacheerden, uitzendkrachten, stagiaires en vrijwilligers) en leerlingen binnen CSG Het Noordik noodzakelijk is om hun werk goed te kunnen doen.
- Aan het gebruik van internet risico's verbonden zijn die nopen tot het stellen van gedragsregels.
- Tegen de achtergrond van deze risico's van de werknemers (inclusief stagiaires en vrijwilligers) en leerlingen verantwoord gebruik van internet en e-mail wordt verwacht.
- CSG Het Noordik gerechtigd is tot het geven van voorschriften voor gebruik van internet en e-mail en het nemen van maatregelen ter bevordering van de goede orde in de onderneming (artikel 7:660 BW).
- De onderhavige gedragscode voorschriften en maatregelen bevat zoals hiervoor genoemd.
- CSG Het Noordik gerechtigd is persoonsgegevens te verwerken ten behoeve van de controle op de naleving van deze gedragscode.
- CSG Het Noordik bij de controle de fundamentele rechten en vrijheden van de betrokken werknemer(s) in acht neemt, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer (artikel 8 sub f WBP).

heeft CSG Het Noordik met instemming van de medezeggenschapsraad op 7 juni 2004 de volgende gedragscode vastgesteld.

Gedragscode internet- en e-mailgebruik

1. Werkingssfeer

Deze regeling is van toepassing op alle geheel of gedeeltelijk geautomatiseerde verwerkingen van persoonsgegevens van personen in dienst van of werkzaam voor of leerling van CSG Het Noordik

2. Uitgangspunten

2.1 De controle op persoonsgegevens over e-mail en internetgebruik is een verwerking van persoonsgegevens in de zin van de Wet Bescherming Persoonsgegevens (WBP).
Toelichting: De WBP kent een ruime betekenis toe aan het begrip 'verwerking van persoonsgegevens'. Hieronder wordt verstaan: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending,

verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens. Een persoonsgegeven in de zin van de WBP is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Het kan om allerlei soorten informatie gaan: om eigenschappen van de betrokkene, diens opvattingen of gedragingen. Meer in het algemeen gaat het om gegevens die bepalend kunnen zijn voor de manier waarop de betrokken persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld.

2.2 De controle op e-mail- en internetgebruik binnen CSG Het Noordik zal conform deze regeling worden uitgevoerd. Indien er zich situaties voordoen waarin deze regeling niet voorziet, zal conform het arbeidsrechtelijk kader en de WBP en in overleg met de medezeggenschapsraad gehandeld worden.

2.3 Gestreefd wordt naar een goede balans tussen verantwoord e-mail- en internetgebruik en bescherming van de privacy van werknemers op de werkplek.

2.4 Persoonsgegevens over e-mail en internetgebruik worden niet langer bewaard dan noodzakelijk, met een maximum bewaartermijn van 6 maanden.

2.5 De werkgever treft voorzieningen over de positie en integriteit van de systeembeheerder en/of afdeling I&A en de controle daarop.

3. Doel

3.1 Deze gedragscode bevat regels ten aanzien van verantwoord e-mail- en internetgebruik en over de wijze waarop controle op persoonsgegevens over e-mail- en internetgebruik plaatsvindt.

3.2 De controle op persoonsgegevens over e-mail en internetgebruik vindt plaats met als doel:

a. Voorkomen van negatieve publiciteit
b. Tegengaan van seksuele intimidatie
c. Controle op bedrijfsgeheimen
d. Systeem en netwerkbeveiliging
e. Kosten en capaciteitsbeheersing
f. Tegengaan van discriminatie

4. E-mailgebruik

4.1 Het e-mail systeem wordt voor zakelijk gebruik beschikbaar gesteld. Gebruik is derhalve verbonden aan taken die voortvloeien uit de functie.

4.2 Beperkt persoonlijk gebruik van het e-mailsysteem is evenwel toegestaan, mits dit niet storend is voor de dagelijkse werkzaamheden en het computernetwerk en dit geen verboden gebruik in de zin van artikel 5 oplevert.

5. Verboden e-mailgebruik

5.1 Het is niet toegestaan om het e-mailsysteem te gebruiken voor het verzenden van berichten met een pornografische, racistische, discriminerende, beledigende of aanstootgevende inhoud.

5.2 Het is niet toegestaan om het e-mailsysteem te gebruiken voor het verzenden van berichten met een (seksueel) intimiderende inhoud.

5.3 Het is niet toegestaan om het e-mail systeem te gebruiken voor het verzenden van berichten die (kunnen) aanzetten tot haat en/of geweld, het deelnemen aan een systeem van kettingbrieven en het versturen van e-mailberichten met een dreigende inhoud.

6. Internetgebruik

6.1 Internetsysteem wordt voor zakelijk gebruik beschikbaar gesteld. Gebruik is derhalve verbonden met taken die voortvloeien uit de functie en het onderwijsproces.

6.2 Beperkt persoonlijk gebruik van het internet is evenwel toegestaan, mits dit niet storend is voor de dagelijkse werkzaamheden en het computernetwerk en dit geen verboden gebruik in de zin van artikel 7 oplevert.

7. Verboden internetgebruik

7.1.1 Het is niet toegestaan om op internet sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten of die in strijd zijn met de wet of onethisch handelen. Noch is het toegestaan dergelijk materiaal, software en applicaties te downloaden.

7.2 Het is niet toegestaan om zich ongeoorloofd toegang tot niet openbare bronnen op internet te verschaffen.

8. Voorwaarden voor controle

8.1 Controle van persoonsgegevens over e-mail- en internetgebruik vindt slechts plaats in het kader van de in artikel 3.2 genoemde doelen.

8.2 Controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot identificeerbare personen.

8.3 Indien een persoon of een groep personen wordt verdacht van het overtreden van regels, kan gedurende een vastgestelde (korte) periode gerichte controle plaatsvinden.

8.4 Controle beperkt zich in beginsel tot verkeersgegevens van het e-mail- en internetgebruik. Slechts bij zwaarwegende redenen vindt controle op de inhoud plaats door de afdeling I&A, uitsluitend in opdracht van de algemeen directeur.

8.5 Verboden e-mail- en internetgebruik wordt zo veel mogelijk softwarematig onmogelijk
gemaakt. Overige controle vindt slechts steekproefsgewijs plaats.

8.6 Bij constatering van verboden gebruik wordt dit onmiddellijk met de betrokkene besproken. De betrokken persoon wordt gewezen op de consequenties wanneer hij niet stopt met het verboden gebruik.

9. Controle

9.1 De controle ter voorkoming van negatieve publiciteit en seksuele intimidatie en de controle in het kader van systeem- en netwerkbeveiliging vindt zo mogelijk plaats op basis van content-filtering. Verdachte berichten worden in dat geval automatisch teruggestuurd naar de afzender.

9.2 De controle op het uitlekken van bedrijfsgeheimen vindt zo mogelijk plaats op basis van steekproefsgewijze content-filtering. Verdachte berichten worden apart gezet voor nader onderzoek.

9.3 De controle in het kader van kosten- en capaciteitsbeheersing wordt beperkt tot verkeersgegevens.

10. Rechten van de personen in dienst van, werkzaam voor of leerling van CSG Het Noordik

10.1 CSG Het Noordik informeert de betrokkene voorafgaand aan de controle op persoonsgegevens over e-mail en internetgebruik, omtrent de doeleinden, de aard van de gegevens, de omstandigheden waaronder zij verkregen zijn en de inhoud van deze regeling.

10.2 De betrokkene kan zich tot CSG Het Noordik wenden met het verzoek voor een volledig overzicht van zijn bewerkte persoonsgegevens. Het verzoek wordt binnen 4 weken beantwoord.

10.3 De betrokkene kan CSG Het Noordik verzoeken zijn persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen indien deze feitelijk onjuist zijn, voor het doel onvolledig of niet ter zake dienend zijn, dan wel in strijd met een wettelijk voorschrift zijn. Het verzoek wordt binnen 4 weken beantwoord.

11. Sancties bij overtreding

Indien de gedragscode door een personeelslid (inclusief gedetacheerden, uitzendkrachten, stagiaires en vrijwilligers) niet wordt nageleefd kan het bestuur voor werknemers de maatregelen treffen zoals genoemd in de artikelen 4.a.7 en 4.a.8 van de de CAO-VO 2003-2005.
Indien de gedragscode door een leerling niet wordt nageleefd kan het bestuur de maatregelen treffen zoals genoemd in hoofdstuk 8 van het leerlingenstatuut.

12. Slotbepaling

CSG Het Noordik kan deze gedragscode met instemming van de medezeggenschapsraad wijzigen of intrekken.

Toelichting per artikel

Algemeen
De invoering van een gedragscode voor het gebruik van e-mail en internet is een besluit waarvoor de instemming van de ondernemingsraad nodig is (artikel 27 lid 1 sub l WOR). De door het CNV gepresenteerde modelgedragscode is een handreiking die aan de specifieke situatie van een onderneming kan worden aangepast. In deze toelichting staan ook andere voorbeelden van verboden e-mail- en internetgebruik en van verantwoord gebruik van het e-mail- en internetsysteem. Zie hiervoor de toelichting bij de navolgende artikelen 4 tot en met 7. Afhankelijke van de organisatie, werkzaamheden of het bedrijfsrisico, kan gebruik van het e-mail- en internetsysteem in meer of mindere mate worden beperkt. Hierbij is het uiteraard van belang, dat vooraf bekend is wat wel en wat niet is toegestaan. Wanneer de werkgever een controlemaatregel wil invoeren dient hij eerst het doel voor de controlemaatregel bekend te maken. Voorbeelden hiervoor zijn genoemd in artikel 3 van de Gedragscode. Maar let op: deze opsomming is zeker niet limitatief.

Artikel 1
Deze gedragscode is van toepassing op (geheel of gedeeltelijke) geautomatiseerde verwerking van persoonsgegevens van personen in dienst van of werkzaam voor de onderneming. Hieronder vallen niet alleen de personen, die een arbeidsovereenkomst hebben met de onderneming, maar ook de personen die bij de onderneming zijn gedetacheerd, uitzendkrachten, stagiaires, vrijwilligers etc.

Artikel 2
De hoofdregel van de Wet Bescherming Persoonsgegevens eist dat persoonsgegevens op behoorlijke en zorgvuldige wijze en in overeenstemming met de wet worden verwerkt. De WBP kent een ruime betekenis toe aan het begrip ‘verwerking van persoonsgegevens’. Hieronder wordt verstaan: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens. Een persoonsgegeven in de zin van de WBP is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Het kan om allerlei soorten informatie gaan: om eigenschappen van de betrokkene, diens opvattingen of gedragingen. Meer in het algemeen gaat het om gegevens die bepalend kunnen zijn voor de manier waarop de betrokken persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld.

Artikel 3
Persoonsgegevens mogen slechts voor bepaalde en gerechtvaardigde doeleinden worden verzameld en niet worden verwerkt voor doeleinden die daarmee onverenigbaar zijn. De werkgever (verantwoordelijke) moet de doelen bepalen vóórdat hij begint met het verwerken van persoonsgegevens. Hierbij is van belang dat het doel van de verwerking zo nauwkeurig en volledig mogelijk wordt omschreven. Als er meerdere doelstellingen zijn, moeten deze afzonderlijk worden genoemd en getoetst op de noodzaak om persoonsgegevens te verzamelen. In overleg met de ondernemingsraad moet worden vastgesteld welke doeleinden voor controle van e-mail en internetgebruik noodzakelijk zijn voor de eigen organisatie. De privacybelangen van de werknemers horen hierbij meegewogen te worden.
De doeleinden, die in artikel 3.2 worden genoemd, zijn voorbeelden van de meest voorkomende doeleinden voor controle op e-mail-en internetgebruik. De hier genoemde voorbeelden zijn uiteraard niet limitatief. Hieronder volgt enige toelichting:

a. begeleiding en individuele beoordeling

In het kader van begeleiding of individuele beoordeling van werknemers kan controle op de inhoud van zakelijke e-mail aan de orde zijn. Deze controle moet verband houden met de taken van de werknemer. Indien een medewerker (mede) tot taak heeft om per e-mail met klanten te communiceren, kan hij aan een steekproefsgewijze inhoudelijke controle onderworpen worden. De controle die wordt uitgevoerd in het kader van deze doelstelling dient zich uitsluitend te richten op zakelijke e-mail en mag niet structureel van aard zijn. Indien de werkgever geen bezwaren heeft tegen het gebruik van het e-mailsysteem voor privé-doeleinden, is het vanuit het oogpunt van bescherming van de persoonlijke levenssfeer van de werknemers wenselijk om de zakelijke mail van de privé-mail te scheiden. Indien scheiding tussen zakelijke en privé-mail onmogelijk blijkt, dient de werkgever de privé-mail zoveel mogelijk te ontzien.

b. Voorkomen van negatieve publiciteit

Werknemers kunnen via e-mail de goede naam van een organisatie behoorlijk aantasten. Het plegen van strafbare feiten, seksuele intimidatie of discriminerende uitingen geschiedt immers onder gebruikmaking van het e-mailadres van de organisatie. Het verdient de voorkeur hier de controle geheel geautomatiseerd te laten plaatsvinden middels content-filtering. Verdachte berichten – zowel inkomende als uitgaande – dienen zoveel mogelijk (geautomatiseerd) te worden teruggestuurd naar de afzender, waardoor vastlegging van de inhoud van het bericht niet nodig is.
Bij gebruik van het internetverkeer via vaste IP-adressen kan een bezoek aan een bepaalde internet-site altijd herleid worden tot een bepaalde organisatie. Om negatieve publiciteit te voorkomen, kan de werkgever het internetgebruik steekproefsgewijs controleren, mits deze doelstellingen reeds van te voren is vastgelegd en in de onderneming bekend is gemaakt.

c. Tegengaan van seksuele intimidatie

Via e-mail kan eenvoudig seksuele intimidatie worden gepleegd. Zowel de inhoud van het bericht als de bijlagen kunnen seksueel intimiderend zijn. Een werkgever die het beleid hiervoor wil handhaven, kan inkomende berichten onderwerpen aan een geautomatiseerde controle. De tekst kan gescand worden op verboden woorden en kunnen verdachte berichten (geautomatiseerd) teruggestuurd te worden aan de oorspronkelijke afzender. Op die wijze kan de privacy van de werknemers ongeschonden blijven.

d. Controle op bedrijfsgeheimen

Controle op het uitlekken van bedrijfsgeheimen via e-mail en internet zal zoveel mogelijk moeten geschieden via geautomatiseerde controle middels content-filtering.

e. Systeem en netwerkbeveiliging

Vanuit beveiligingsoogpunt is het wenselijk om e-mail te controleren. Het kan dan gaan om het tegengaan van systeemaanvallen door virussen of andere schadelijke programma's. Bij deze controle verdient een geheel geautomatiseerde controle van inkomende berichten en bijlagen de voorkeur. Indien een besmet bericht gevonden wordt, kan dit op een aparte locatie worden bewaard voor nader onderzoek en eventuele herstelwerkzaamheden.

f. Kosten en capaciteitsbeheersing

Uiteraard kost het versturen van e-mail geld en legt het beslag op de beschikbare capaciteit van het netwerk. Het kostenaspect is met name aan de orde als de e-mailverbinding via de telefoon loopt. Deze vorm van controle kan beperkt blijven tot het controleren van de verkeersgegevens. Kennisneming van de inhoud van de mail is voor dit doel niet noodzakelijk.

g. Tegengaan van discriminatie

Zie sub c.

Artikel 4
In de gedragscode kunnen gedragsregels worden opgenomen over wat er in een organisatie onder verantwoord e-mailgebruik wordt verstaan. Een totaal verbod op het versturen en ontvangen van persoonlijke e-mailberichten is niet mogelijk. De organisatie kan wel beperkende voorwaarden opstellen aan het persoonlijk gebruik van het e-mailsysteem. Hieronder een aantal andere opties:

- Werknemers mogen het e-mailsysteem gebruiken voor het ontvangen en versturen van e-mailberichten mits dit beperkt blijft tot …minuten per dag/week.
- Werknemers mogen het e-mailsysteem gebruiken voor het ontvangen en versturen van persoonlijke e-mailberichten mits dit niet storend is voor de dagelijkse werkzaamheden en het computernetwerk.
- Werknemers mogen incidenteel en kortstondig het e-mailsysteem gebruiken voor het ontvangen en versturen van persoonlijke e-mailberichten, mits dit niet storend is voor de dagelijkse werkzaamheden en het computernetwerk

Artikel 5
In de gedragscode kunnen gedragsregels worden opgenomen over wat niet toegestaan is bij een verantwoord e-mailgebruik. Andere voorbeelden van verboden gebruik zijn:

- Het versturen en ontvangen van kettingbrieven.
- Het versturen van e-mailberichten met een dreigende inhoud.

Artikel 6
In de gedragscode kunnen gedragsregels worden opgenomen over wat er in de organisatie onder verantwoord internetgebruik wordt verstaan. Hieronder een aantal andere opties:

- Voor het gebruik van het internetsysteem voor persoonlijke doeleinden stelt de organisatie een aparte computer beschikbaar, die zich (…plaats invullen….) bevindt. Het is niet toegestaan om de computer op de eigen werkplek hiervoor te gebruiken.
- Werknemers mogen het internetsysteem voor persoonlijke doeleinden gebruiken, mits dit beperkt blijft tot … minuten per dag/week.
- Werknemers mogen het internetsysteem voor persoonlijke doeleinden gebruiken, mits dit niet storend is voor de dagelijkse werkzaamheden en het computernetwerk.
- Werknemers mogen incidenteel en kortstondig het internetsysteem voor persoonlijke doeleinden gebruiken, mits dit niet storend is voor de dagelijkse werkzaamheden en het computernetwerk.

Een totaal verbod op het internetgebruik voor persoonlijke doeleinden is niet mogelijk.

Artikel 7
In de gedragscode kunnen regels worden opgenomen over wat niet is toegestaan bij een verantwoord internetgebruik. Hieronder een aantal andere opties:

- Op internet in strijd met de wet of onethisch handelen.
- Software en applicaties downloaden.
- Et cetera.

Artikel 8
8.6. Wanneer de werkgever constateert dat een werknemer zich schuldig maakt aan verboden gebruik van het e-mail- en/of internetsysteem, bespreekt hij dit onmiddellijk met de betrokken werknemer. Daarbij wordt de werknemer gewaarschuwd voor de (rechtspositionele) consequenties die het verboden gebruik van het e-mail- en/of internetsysteem voor hem kan hebben.

Artikel 10
De betrokken werknemer heeft het recht zich vrijelijk en met redelijke tussenpozen tot zijn werkgever te wenden met het verzoek hem mede te delen of hem betreffende persoonsgegevens worden verwerkt. De werkgever deelt de betrokkene schriftelijk binnen vier weken mee of hem betreffende persoonsgegevens worden verwerkt

De betrokken werknemer kan de werkgever verzoeken de hem betreffende persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen indien deze gegevens

- onjuist zijn,
- voor het doel of de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn,
- dan wel anderszins in strijd met een wettelijk voorschrift of met deze gedragscode zijn verwerkt.

De werkgever bericht de verzoeker (werknemer) binnen vier weken na ontvangst van het verzoek schriftelijk in hoeverre hij aan het verzoek zal voldoen. Een weigering is met redenen omkleed. De werkgever draagt er zorg voor, dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd.

[www.noordik.nl – alle_bestanden/gedragscode_internet.pdf]