

Surfing in the workplace van VNO-NCW

Het volgende stuk over Internet gebruik komt uit de folder van VNO NCW 'Surfing in the workplace' uit 2001 en omdat wij het niet beter kunnen vertellen kunt u het hier in zijn geheel lezen.

Inleiding: Het gebruik van e-mail en internet in bedrijven neemt een hoge vlucht. En daarmee wordt de vraag actueel hoe bedrijven en werknemers met de nieuwe communicatiemiddelen moeten omgaan. Wat mag wel en wat mag niet? Mag een werknemer vanaf zijn werkplek ook persoonlijke e-mailtjes versturen en heeft een werkgever het recht om het internet- en e-mailgebruik van zijn personeel te controleren? En hoe zit het dan met de Wet Bescherming Persoonsgegevens?

- Gebruiksaanwijzing 'Modelgedragscode internet- en e-mailgebruik'
- 1. Zorg dat iedereen de regeling kent,
- 2. De inhoud van de regeling
- 3. De wijze van invoering van de gedragscode
- 4. Verbod privé-gebruik
- 5. Sacties
- Modelgedragscode internet- en e-mailgebruik
- Adressen

De Modelgedragscode internet- en e-mailgebruik geeft ondernemingen een handvat om deze vragen voor hun bedrijf te beantwoorden. De modelgedragscode is als tekstbestand beschikbaar in deze folder **Modelgedragscode**, maar ook via internet, www.vno-ncw.nl

Gebruiksaanwijzing 'Modelgedragscode internet- en e-mailgebruik'

De concepttekst van de gedragscode kan, na invulling van de bedrijfsnaam en instemming met de tekst door de ondernemingsraad, van kracht worden verklaard voor alle medewerkers. Aanbevolen wordt de volgende aspecten in het oog te houden:

1. Zorg dat iedereen de regeling kent,

en denk bijvoorbeeld ook aan levering aan iedere werknemer op papier, via e-mail, publicatie in een huisorgaan, meldtekst op het scherm. Opnemen in het personeelsreglement is te zijner tijd uiteraard nodig.

Jaarlijks worden de resultaten van controles met de ondernemingsraad besproken. Ook wordt dan bezien of de regeling nog up-to-date is en bijvoorbeeld vanuit technisch oogpunt aanpassing behoeft. Deze wijzigingen horen op dezelfde wijze bekendgemaakt te worden als de oorspronkelijke gedragsregels.

2. De inhoud van de regeling

De regeling gaat over het gebruik van internet en e-mail. Een belangrijk punt is de totstandkoming van een goede balans tussen verantwoord gebruik en bescherming van de privacy van de medewerkers op de werkplek. De tekst van de Modelgedragscode sluit op dat punt aan bij de Wet Bescherming Persoonsgegevens. Een algemene brochure over deze wet is verkrijgbaar (en te raadplegen) bij het ministerie van Justitie (www.minjust.nl) of bij VNO-NCW (www.vno-ncw.nl/privacy). Een specifieke brochure

over internetgebruik op de werkplek is bij het College Bescherming Persoonsgegevens (www.registratiekamer.nl) op te vragen.

Ook beveiliging van informatievoorziening en informatiesystemen komt op enkele punten aan de orde. Daaromtrent zijn uiteraard veel uitvoeriger maatregelen voorstelbaar dan hier aangestipt. Onder andere de Code voor Informatiebeveiliging (www.nni.nl) geeft hierin inzicht.

3. Wijze van invoering van de gedragscode

Invoering van een gedragscode kan volgens het volgende traject verlopen:

- a. Verzamel en analyseer de huidige formele en informele regels in het bedrijf ten aanzien van internetgebruik, waaronder begrepen het afschermen van bepaalde websites, het gebruik van e-mail, het benutten van disclaimers aan het eind van de e-mailberichten, etc.;
- b. Bespreek het onderwerp met de ondernemingsraad; Stel een conceptregeling op en leg deze voor aan de ondernemingsraad. Toelichting: Op grond van art. 27, lid 1, sub k, van de Wet op de ondernemingsraden (WOR) is instemming vereist voor de vaststelling, wijziging of intrekking van een regeling omtrent de registratie van, de omgang met en de bescherming van de persoonsgegevens van de in de onderneming werkzame personen. Het gaat hierbij inderdaad om zo'n regeling. Ook is instemming vereist (art. 27, lid 1, sub 1, WOR) voor een besluit tot vaststelling, wijziging of intrekking van een regeling inzake voorzieningen die gericht zijn op of geschikt zijn voor waarneming van of controle op aanwezigheid, gedrag of prestaties van de in de onderneming werkzame personen. Het instemmingsrecht van de OR betreft dus zowel de reglementering van een voorziening als de voorziening zelf. Voorbeelden van een dergelijke voorziening zijn: prikklok, pieper, controlecamera's, beveiligingscamera's, chipkaarten, telefoonrecording.
- c. De controle door registratie van het gebruik van internet moet worden gemeld bij het College Bescherming Persoonsgegevens (CBP) voordat met de gegevensverwerking wordt begonnen, omdat deze niet valt onder het Vrijstellingsbesluit. Dit registreren kan elektronisch op de website van het CBP (www.registratiekamer.nl) of via een daar op te vragen formulier.

4. Verbod privé-gebruik

De hier voorgestelde regeling verbiedt privé-gebruik. Vaak ontbreekt immers de noodzaak om tijdens werktijd contact te zoeken met de buitenwereld (zoals bij de telefoon), waardoor het eigenlijk nooit echt noodzakelijk zal zijn internet vanaf de werkplek te gebruiken voor privé-doelen. Uiteraard kan overwogen worden om privé-gebruik toch in zekere mate toe te staan.

Dan zal de werkgever er rekening mee dienen te houden dat bij controle van de regeling het persoonlijk berichtenverkeer in beginsel moet worden gerespecteerd. Ook zal dan bijvoorbeeld stilgestaan moeten worden bij de vraag hoe te handelen met de categorie internetdiensten voor privé-gebruik waarvoor betaald moet worden.

Overwogen kan ook worden op een algemeen toegankelijke plaats binnen de onderneming een speciale toegang, los van de bedrijfsmatige toegang, ter beschikking van de medewerkers te stellen.

Bij toestaan van enig privé-gebruik, kan bijvoorbeeld de volgende tekst in de modelgedragscode ingevoegd worden (in 3.3 de eerste alinea vervangen, en in de tweede het woord 'onacceptabel' invoegen voor 'persoonlijk'):

'Werknemers mogen internet en e-mail incidenteel en kortstondig voor privé-doeleinden gebruiken, zowel intern als extern, mits dit niet storend is voor de dagelijkse werkzaamheden en mits hierbij voldaan wordt aan de verdere richtlijnen van deze gedragscode'.

In dat geval past een extra alinea onder 'Controle', als aanvulling op 4.3: 'Controleren alsmede openen van e-mail, ook die voor privé-gebruik, ten behoeve van het opsporen van onrechtmatig gedrag van de werknemer is dus toegestaan indien er sprake is van een redelijke verdenking of een vermoeden van ongeoorloofd handelen'.

5. Sancties

Overwogen kan worden, afhankelijk van het bestaande ondernemingsbeleid, concreet aan te geven welke sancties worden toegepast bij bepaalde overtredingen.

Modelgedragscode internet- en e-mailgebruik

Overwegingen

Deze tekst omschrijft het gebruik van internet en e-mail voor (naam onderneming).

De volgende punten zijn overwogen bij het vaststellen van deze gedragscode:

1. Gebruik van het internet en e-mail is voor velen binnen (naam) nodig om het werk goed te doen. Maar onjuist hiermee omgaan kost tijd en capaciteit van mensen en apparatuur, en brengt diverse risico's met zich mee.
2. Internet kent verschillende verschijningsvormen. Dit zijn onder andere e-mail (via internet en via intranet), World Wide Web (surfen), File Transfer (bestandsuitwisseling), Usenet (nieuwsgroepen) en chat (babbelbox). Aan het gebruik van het internet zijn, per verschijningsvorm, risico's verbonden die nopen tot het stellen van gedrags- en gebruiksregels. Bij risico's valt te denken aan beschadiging van het netwerk door virussen, uitlekken van bedrijfsgeheimen en het in diskrediet brengen van de goede naam van de onderneming.
3. Ter vermijding van dergelijke risico's kan (naam onderneming) voor schriften geven voor het verrichten van de arbeid, en maatregelen nemen ter bevordering van de goede orde in de onderneming. De hierna weergegeven regels vallen onder deze bepaling.
4. Tegen de achtergrond van de risico's van het gebruik van internet en e-mail wordt van de gebruiker professioneel en integer handelen verwacht.
5. Het gebruik van internet en e-mail wordt vastgelegd. Deze registratie geschiedt om de continuïteit van de technische infrastructuur te waarborgen, verstoring van bedrijfsprocessen en andere (financiële) schade tegen te gaan en om toezicht te houden op de naleving van de gedrags- en gebruiksregels door de gebruiker.

6. Inhoudelijke controle van het internet- en e-mailgebruik kan plaatsvinden indien sprake is van een vermoeden van strijd met de gedrags- en gebruiksregels door de gebruiker. Niet naleving van deze regels kan leiden tot disciplinaire en arbeidsrechtelijke maatregelen.

7. Deze gedragscode omtrent internet en e-mail betreft:
de regels die de werknemer dient na te leven bij het gebruiken van de door (naam) voor zakelijk gebruik ter beschikking gestelde internet- en e-mailsystemen;
de omstandigheden waaronder (naam) besluit tot het registreren, verzamelen en monitoren van tot personen herleidbare data omtrent internet- en e-mailgebruik.

1. Werkingssfeer

1.1 Deze regeling geldt voor een ieder die voor (naam onderneming) werkzaam is.

2. Algemeen

2.1 (naamonderneming) behoudt zich het recht voor om de toegang tot bepaalde sites te beperken. Met name sites met een pornografische, racistische, discriminerende of een op entertainment gerichte inhoud zullen (kunnen) worden geweerd.

2.2 (naam onderneming) kan het recht tot gebruik van (een deel van) internet toestaan, maar ook altijd weer intrekken. Zonder dat recht is gebruik van (een deel van) internet niet toegestaan.

2.3 De gebruikelijke gedragsregels, zoals de regels die momenteel gelden voor het ondertekenen van schriftelijke correspondentie, het vertegenwoordigen van (naam onderneming) en voor het verzenden van post (zoals correct taalgebruik) zijn ook van toepassing op e-mail en andere toepassingen (zoals nieuwsgroepen, telefoneren via internet).

3. Gebruik

3.1 Medewerkers van (naam onderneming) mogen uitsluitend zakelijk (of naar keuze: beperkt persoonlijk) gebruikmaken van internet. Gebruik is dus verbonden met taken/bezigheden die voortvloeien uit de functie. Daarbij dienen zij zich te houden aan de door (naam onderneming) opgestelde regels en procedures.

3.2 De infrastructuur voor elektronische communicatie kent een eigen vorm van kwetsbaarheid, en een eigen vorm van beveiliging. Deze vraagt om speciale aandacht op tenminste de volgende punten:

user-identificatie (inlog-naam) en wachtwoord zijn persoonsgebonden en mogen niet aan anderen worden doorgegeven;
het downloaden van software en applicaties is niet toegestaan, tenzij vooraf schriftelijke toestemming is verleend door (invullen, bijvoorbeeld het hoofd van de informatievoorziening automatiseringsafdeling). Deze toestemming wordt alleen verleend als wordt voldaan aan de geldende rechten en eventuele licenties worden betaald. Gedownloade software en applicaties moeten op virussen zijn gescand voor gebruik;

vertrouwelijke gegevens en bedrijfsgevoelige informatie mogen niet zonder toestemming naar buiten de organisatie worden verstuurd. Het berichtenverkeer hoort dan versleuteld te verlopen;
het is niet toegestaan inkomende privé-berichten te genereren door deel te nemen aan niet-zakelijke nieuwsgroepen, abonnementen op e-zines, nieuwsbrieven en dergelijke. Onbedoelde inbreuken op beveiliging, van binnenuit of vanuit de buitenwereld, dient u aan de systeembeheerderautomatiseringsafdeling te melden.

3.3 Het is niet toegestaan om voor persoonlijke doeleinden internet te gebruiken. De werknemer die niet-zakelijke e-mail ontvangt, behoort de verzender te vragen om de verzending daarvan te stoppen. Bij persoonlijk gebruik van internet moet onder andere worden gedacht aan het spelen of downloaden van spelletjes, winkelen, gokken of deelnemen aan kansspelen en het bezoeken van chat-/babbelboxen.

3.4 Het is in het bijzonder niet toegestaan om op internet:

sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten;
pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal te bekijken of te downloaden;
zich ongeoorloofd toegang te verschaffen tot niet openbare bronnen op het internet;
opzettelijk informatie waartoe men via internet toegang heeft verkregen zonder toestemming te veranderen of te vernietigen. Indien u ongevraagd informatie van deze aard krijgt aangeboden, dient u dat aan (het hoofd automatisering) te melden.

3.5 Het is bovendien niet toegestaan om door middel van e-mail:

dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende berichten en kettingmailberichten te verzenden of door te sturen;
iemand elektronisch lastig te vallen.
Indien u ongevraagd informatie van deze aard aangeboden krijgt, dient u dit te melden aan (het hoofd van de automatiseringsafdeling).

3.6 Het is ook anderszins niet toegestaan op internet in strijd met de wet of onethisch te handelen.

4. Controle

4.1 Om de veiligheid van het netwerk te waarborgen en toe te zien op een zorgvuldig gebruik overeenkomstig deze regeling, worden van tijd tot tijd controles uitgevoerd. Hiernaast wordt toegezien op de technische integriteit en beschikbaarheid van de infrastructuur en diensten. Het toezicht op het gebruik zal bestaan uit het steekproefsgewijs controleren van het gebruik van internet en e-mailverkeer (tijdsbesteding, sites die bezocht worden). Daartoe kunnen anonieme lijsten van bezochte internetsites en van verstuurde e-mails worden uitgedraaid.

4.2 Binnenkomende internet- en e-mailverkeer wordt zo goed mogelijk gecontroleerd op virussen en soortgelijk ongerief. Mocht blijken dat een e-mailbericht een virus bevat, dan wordt het automatisch tegengehouden en worden de verzender en ontvanger daarover

ingelicht. Indien desondanks een e-mail wordt ontvangen dat mogelijk een virus bevat, dan dient de ontvanger onverwijld contact op te nemen met (het hoofd automatisering).

4.3 Indien mocht blijken dat in strijd met deze regeling wordt gehandeld of indien daarvoor aanwijzingen zijn (zoals klachten, signalen van binnen of buiten de organisatie en systeemstoringen), dan kunnen gegevens van (de) betrokken gebruiker(s) worden uitgedraaid, bekeken en gebruikt.

4.4 De betreffende gegevens worden bewaard zolang dit in het kader van nader onderzoek en eventueel te treffen maatregelen jegens een gebruiker noodzakelijk is.

5. Sancties

5.1 Bij handelen in strijd met deze regeling, het bedrijfsbelang of de algemeen geldende normen en waarden voor het gebruik van internet, kunnen afhankelijk van de aard en de ernst van de overtreding maatregelen worden getroffen. Hierbij gaat het om disciplinaire en arbeidsrechtelijke maatregelen zoals berisping, overplaatsing, schorsing en beëindiging van de arbeidsovereenkomst.

6. Slot

6.1 In alle gevallen waarin deze regeling niet voorziet, beslist de directie van (naam onderneming).

6.2 Deze regeling treedt in werking (datum)

Adressen

Vereniging FME-CWM

De Vereniging FME-GWM is de bedrijfstakorganisatie voor de metaal- kunststof-, elektronica- en elektrotechnische industrie. De 2.850 aangesloten bedrijven hebben een gezamenlijke jaaromzet van 75 miljard gulden (waarvan 50 miljard uit export) en bieden werk aan ruim 300.000 personen. Bij FME-CWM zijn 145 brancheorganisaties gehuisvest. De Vereniging FME-CWM heeft regionale kantoren in Apeldoorn, Barendrecht, Haren (Gn), Tilburg en Uithoorn.

FME-GWM
Postbus 190, 2700 AD Zoetermeer
Telefoon 079 353 11 00
Fax 079 353 13 65
Helpdesk 0900 821 21 91
Internet www.fme.nl

Vereniging VNO-NCW

De Vereniging VNO-NGW is de grootste centrale ondernemingsorganisatie van Nederland. Zij behartigt de gemeenschappelijke belangen van 150 brancheverenigingen met hun ruim 80.000 aangesloten ondernemingen. De vijf hij VNO-NGW aangesloten regionale werkgeversverenigingen en Jong Management vertegenwoordigen 8.500 persoonlijke leden. VNO-NCW representeert 80 procent van de werkgelegenheid in de marktsector.

Postbus 93002, 2509 AA Den Haag

Telefoon 070 349 03 49

Fax 070 349 03 00

Antwoordnummer VNO-NCW 070 349 03 66 (telefonische vraagbaak voor leden)

Internet www.vno-ncw.nl

Hoewel bij de samenstelling van deze brochure grote zorgvuldigheid is betracht, kunnen de samenstellers geen aansprakelijkheid aanvaarden voor schade, van welke aard ook, die het directe of indirecte gevolg is van handelingen en/of beslissingen die (mede) gebaseerd zijn op de informatie in deze brochure.