Helpt je verder

Gedragscode voor het gebruik van e-mail, internet en social media

Eigenaar: M. de Vos
Documentbeheer: R. Kok
Vastgesteld: 04-10-2016

Jeugdformaat

De Raad van Bestuur van Stichting Jeugdformaat, gevestigd te Rijswijk heeft,

Gelet op:

- Artikel 7:611 en 7:660 van het Burgerlijk Wetboek;
- De Wet Bescherming Persoonsgegevens;
- Artikel 27 lid 1 sub k en l Wet op de Ondernemingsraden.

Overwegende dat:

- De Stichting Jeugdformaat en haar werknemers zich ten opzichte van elkaar dienen te gedragen als een goed werkgever en een goed werknemer (art. 7:611 BW).
- Het gebruik van e-mail, social media en internet voor (veel van) de werknemers binnen Stichting Jeugdformaat noodzakelijk is om hun werk goed te kunnen doen.
- Aan het gebruik van e-mail, social media en internet risico's verbonden zijn die nopen tot het stellen van gedragsregels.
- Tegen de achtergrond van deze risico's van de werknemers verantwoord gebruik van e-mail, social media en internet wordt verwacht.
- Stichting Jeugdformaat gerechtigd is tot het geven van voorschriften voor gebruik van e-mail, social media en internet 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.
- Stichting Jeugdformaat gerechtigd is persoonsgegevens te verwerken ten behoeve van de controle op de naleving van deze gedragscode.
- Stichting Jeugdformaat 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)

per 4 oktober 2016 de volgende gedragscode vastgesteld.

Inleiding

E-mail, internet en social media zijn een vast onderdeel van ons werk, stellen ons in staat om altijd op de hoogte te zijn van de laatste ontwikkelingen en zorgen dat we snel met anderen kunnen communiceren. Daarmee rijst de vraag hoe om te gaan met deze communicatiemiddelen. Wat mag wel en wat mag niet? Medewerkers van Jeugdformaat mogen e-mail, internet en social media gebruiken mits de organisatie er niet onder lijdt.

Deze gedragscode geeft de wijze aan waarop binnen Jeugdformaat wordt omgegaan met e-mail, internet en social media, bevat regels voor verantwoord gebruik hiervan en geeft de wijze van controle op deze regels aan. Gestreefd wordt naar een goede balans tussen verantwoord e-mail, social media en internetgebruik en bescherming van de privacy van cliënten en medewerkers. Het Jeugdformaat protocol “Omgang met cliëntgegevens” en het “Privacyreglement Cliënten” geven regels voor een zorgvuldige omgang met persoonsgegevens van cliënten.

Deze gedragscode geldt voor alle medewerkers van Jeugdformaat. Onder medewerkers wordt ook verstaan: tijdelijk personeel, uitzendkrachten, gedetacheerden, stagiair(es), vrijwilligers en externen.

Kortom, de gedragscode geeft grenzen aan waardoor iedere medewerker goed in staat is om e-mail, internet en social media op een zorgvuldige en verantwoorde manier te gebruiken.

1. Werkingssfeer

Deze regeling is van toepassing op alle geheel of gedeeltelijk geautomatiseerde verwerkingen van persoonsgegevens, als bedoeld in de Wet bescherming persoonsgegevens Artikel 1 lid a., door personen in dienst van of werkzaam voor Jeugdformaat.

2. Uitgangspunten

2.1 De controle op persoonsgegevens over e-mail, social media en internetgebruik is een verwerking van persoonsgegevens in de zin van de Wet Bescherming Persoonsgegevens.

2.2 De controle op e-mail, social media en internetgebruik binnen Jeugdformaat 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 Raad van Bestuur en de ondernemingsraad gehandeld worden.

2.3 Gestreefd wordt naar een goede balans tussen praktisch, nuttig en verantwoord e-mail, social media en internetgebruik, en bescherming van de privacy van cliënten en werknemers.

2.4 Persoonsgegevens over e-mail, social media en internetgebruik worden niet langer bewaard dan noodzakelijk, met een maximum bewaartermijn van 6 maanden. Bij constatering van misbruik volgt een functioneringstraject en worden gegevens over e-mail, social media en internetgebruik in het personeelsdossier opgenomen.

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

3. Doel

3.1 Deze gedragscode bevat regels ten aanzien van verantwoord e-mail, social media en internetgebruik en regels over de wijze waarop controle op persoonsgegevens over e-mail, social media en internetgebruik plaats vindt.

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

a. Begeleiding/individuele beoordeling
b. Voorkomen van negatieve publiciteit
c. Tegengaan van seksuele intimidatie
d. Controle op het delen en verspreiden van bedrijfsgeheimen
e. Systeem en netwerkbeveiliging
f. Kosten en capaciteitsbeheersing
g. Tegengaan van discriminatie

4. E-mailgebruik

4.1 Het e-mail systeem wordt aan de werknemer voor zakelijk gebruik beschikbaar gesteld. Gebruik is derhalve verbonden met 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 dit geen verboden gebruik in de zin van artikel 5 oplevert.

4.3 Bij het versturen van e-mailberichten moet de afzender correct en volgens de huisstijl vermeld worden.

5. Verboden e-mailgebruik

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

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

5.3 Het is de werknemer niet toegestaan om het e-mail systeem te gebruiken voor het verzenden van berichten die (kunnen) aanzetten tot haat en/of geweld.

5.4 Het is de werknemer niet toegestaan om het e-mailsysteem te gebruiken voor het meesturen van bijlagen groter dan 25 megabyte(MB).

5.5 Het is de werknemer niet toegestaan om het e-mailsysteem te gebruiken voor het versturen van berichten naar iemand die er geen wilt ontvangen (“spam” genoemd).

5.6 Het is de werknemer niet toegestaan om het e-mailsysteem te gebruiken voor het versturen van kettingbrieven of berichten die (kunnen) aanzetten tot haat en/of geweld.

5.7 Het is de werknemer niet toegestaan om via privé e-mail over of met cliënten te communiceren of het privé e-mailadres te gebruiken voor uitwisseling van cliëntgegevens.

6. Internetgebruik

6.1 Het internetsysteem wordt aan de werknemer voor zakelijk gebruik beschikbaar gesteld. Gebruik is derhalve verbonden met taken die voortvloeien uit de functie.

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

7. Verboden internetgebruik

7.1 Het is de werknemer niet toegestaan om internetsites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten. Noch is het toegestaan dergelijk materiaal te downloaden en te publiceren en/of uploaden.

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

7.3 Het is de werknemer niet toegestaan om op internet in strijd met de wet of onethisch te handelen.

7.4 Het is de werknemer niet toegestaan om software en/of applicaties te downloaden.

8. Social media gebruik

8.1 Jeugdformaat ondersteunt het belang van sociale media. Het is werknemer toegestaan om onder werktijd actief te zijn op sociale media mits het werk gerelateerde content betreft en het werk hier niet onder lijdt.

8.2 Het is werknemer toegestaan om kennis en informatie te delen, mits het geen vertrouwelijke of privacygevoelige informatie betreft en het Jeugdformaat niet schaadt.

8.3 Het is werknemer toegestaan om via WhatsApp met cliënten te communiceren, mits het geen privacygevoelige informatie of persoonsgegevens betreft. In geval van een conflict van plichten, bijvoorbeeld als de veiligheid van de cliënt of een ander in het geding is, mogen wel persoonsgegevens uitgewisseld worden. Bij twijfel dient de leidinggevende geraadpleegd te worden. De onderbouwing van de afwijking van de regelgeving, alsmede een typering van de gegevens waar het om gaat, wordt vermeld in het cliëntdossier.

8.4 De werknemer is persoonlijk verantwoordelijk voor de inhoud welke hij of zij publiceert op blogs, wiki's, fora en andere media die gebaseerd zijn op user-generated content.

8.5 In geval een online discussie ontspoort of dreigt te ontsporen dient de werknemer direct contact op te nemen met zijn/haar leidinggevende en de afdeling Communicatie om de te volgen strategie te bespreken.

8.6 Bij twijfel of een publicatie de social media richtlijnen schaadt neemt de werknemer contact op met zijn/haar leidinggevende en de afdeling Communicatie.

8.7 Indien de werknemer privé op social media over Jeugdformaat schrijft, dient hij of zij een disclaimer (zie het voorbeeld hieronder) op te nemen waarin staat dat dit het persoonlijke standpunt van de medewerker weergeeft en dat dit niet overeen hoeft te komen met dat van Jeugdformaat.

Voorbeeld disclaimer: *De hier geuite standpunten en meningen zijn de persoonlijke mening van (naam medewerker) en staan los van eventuele officiële standpunten van Stichting Jeugdformaat. Stichting Jeugdformaat is niet verantwoordelijk voor de inhoud van uitlatingen en reacties van derden op de hier gepubliceerde meningen en standpunten.*

9. Verboden social media gebruik

9.1 Het is werknemer niet toegestaan om vertrouwelijke, privacygevoelige of schadelijke informatie te publiceren of anderszins via social media te verstrekken over Jeugdformaat, cliënten, collega's of andere professionele relaties. Hierin wordt geen onderscheid gemaakt tussen informatie over organisaties of personen. In geval van een conflict van plichten, bijvoorbeeld als de veiligheid van een cliënt of een ander in het geding is, mag wel privacygevoelige informatie uitgewisseld worden. Bij twijfel dient de leidinggevende geraadpleegd te worden. De onderbouwing van de afwijking van de regelgeving, alsmede een typering van de gegevens waar het om gaat, wordt vermeld in het cliëntdossier.

9.2 Het is werknemer niet toegestaan om informatie die niet in zijn/haar werk gerelateerde expertisegebied ligt of waarvoor hij/zij niet bevoegd is te publiceren.

9.3 Het is werknemer zonder toestemming niet toegestaan om tekst uit documenten, logo's of beeldmateriaal van Jeugdformaat te publiceren.

9.4 Het is werknemer niet toegestaan om berichten te publiceren die obsceen, bedreigend, discriminerend of haatdragend zijn.

9.5 Het opslaan van cliënt-, bedrijfs- of enige andere vertrouwelijke gegevens bij online opslagdiensten is niet toegestaan. Bij opslag van bestanden bij online opslagdiensten kan niet worden uitgesloten dat onbevoegden inzage krijgen in persoonsgegevens van de cliënt of andere vertrouwelijke gegevens.

9.6 De werknemer dient rekening te houden met het wettelijk vastgelegde beeld-, auteurs- en citaatrecht. Het is verboden om zonder toestemming van de maker andermans werk te publiceren.

10. Voorwaarden voor controle

10.1 Controle in het kader van begeleiding en/of individuele beoordeling vindt alleen plaats in geval van (vermoeden van) misbruik en alleen in opdracht van de Raad van Bestuur.

10.2 Controle van persoonsgegevens over e-mail, social media en internetgebruik vindt slechts plaats in het kader van in artikel 3.2 genoemde doelen.

10.3 Controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot een identificeerbare persoon.

10.4 Indien een werknemer of een groep werknemers wordt verdacht de regels te overtreden, kan gedurende een vastgestelde (korte) periode gerichte controle plaatsvinden.

10.5 Controle beperkt zich in beginsel tot verkeersgegevens van het e-mail, social media en internetgebruik. Slechts bij zwaarwegende redenen, zoals een ernstig vermoeden van misbruik, vindt controle op de inhoud plaats.

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

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

10.8 E-mail berichten van werknemers met een vertrouwensfunctie zijn in beginsel uitgesloten van gericht onderzoek. Onder werknemers met een vertrouwensfunctie worden verstaan:

- Bestuursleden
- Directiesecretaresses Raad van Bestuur

- Leden van de ondernemingsraad (e-mail onderling)
- HR adviseurs
- Hoofd P&O
- Bedrijfsartsen
- Preventiemedewerker
- Vertrouwenspersonen

10.9 Voor het tegengaan van virussen en andere schadelijke programma's, in het kader van systeem- en netwerkbeveiliging, wordt het e-mail en internetgebruik op geautomatiseerde wijze gecontroleerd.

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

11. Rechten van de werknemer

11.1 De werkgever informeert de werknemer voorafgaand aan de controle op persoonsgegevens over e-mail, social media en internetgebruik, omtrent de doeleinden, de aard van de gegevens, de omstandigheden waaronder zij verkregen zijn en de inhoud van deze regeling (artikel 33, WBP).

11.2 De werknemer kan zich tot de werkgever wenden met het verzoek voor een volledig overzicht van zijn persoonsgegevens. Het verzoek wordt binnen 4 weken beantwoord (artikel 35, WBP).

11.3 De werknemer kan de werkgever 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 (artikel 36, WBP).

11.4 De werknemer kan bij de werkgever verzet aantekenen tegen verwerking van zijn persoonsgegevens in verband met bijzondere persoonlijke omstandigheden. De werkgever oordeelt binnen 4 weken na ontvangst van het verzet of dit gerechtvaardigd is. Indien de werkgever het verzet gerechtvaardigd acht, beëindigt hij terstond de verwerking (artikel 40, WBP).

12. Slotbepaling

12.1 De werkgever kan tot invoering, wijziging of intrekking van een gedragscode voor het gebruik van e-mail, social media en internet besluiten met instemming van de ondernemingsraad (artikel 27 lid 1 sub l WOR). Wijzigingen worden schriftelijk vastgelegd en voorafgaand aan de invoering aan de werknemers bekend gemaakt.

12.2 De gedragscode voor het gebruik van e-mail, social media en internet regeling wordt eens per drie jaar geëvalueerd door de werkgever en de ondernemingsraad.

12.3 De gedragscode voor het gebruik van e-mail, social media en internet is tot stand gekomen bij besluit van 4 oktober 2016.

TOELICHTING OP DE GEDRAGSCODE

Algemeen
De invoering van de gedragscode voor het gebruik van e-mail, social media en internet is een besluit waarvoor instemming van de ondernemingsraad nodig is (artikel 27, lid 1, onder l, WOR). De AP (Autoriteit Persoonsgegevens, voorheen College Bescherming Persoonsgegevens) heeft een checklist ontwikkeld die de OR handvatten biedt bij de beoordeling van een dergelijke regeling.

In deze toelichting staan ook andere voorbeelden van verboden e-mail, social media en internetgebruik en van verantwoord gebruik van e-mail, social media en internet. Zie hiervoor de toelichting bij de navolgende artikelen 4 tot en met 9. Afhankelijke van de organisatie, werkzaamheden of het bedrijfsrisico, kan gebruik van het e-mail, social media en internet 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. Deze doelen zijn opgesomd in artikel 3.2.

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. Hier vallen niet alleen de personen onder, 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 ter beschikking stelling, 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.

Uitleg bij 2.2
Controle en gedragsregels ten aanzien van het gebruik van e-mail, social media en internet moet niet los gezien worden van het beleid ten aanzien van andere communicatiemiddelen en controlemaatregelen in de organisatie. Het beleid voor online gedrag moet in overeenstemming zijn met het beleid voor offline gedrag. Niet de technische mogelijkheid van controle, maar de noodzaak dient de vorm en de maat hiervan te bepalen.

Uitleg bij 2.4
De systeembeheerder is als het ware de sleutel tot de persoonsgegevens over het gebruik van e-mail, social media en internet. Vanuit het oogpunt van de privacy is het belangrijk om afspraken te maken over wie in welke gevallen opdracht kan geven over de controle. Ook de geheimhoudingsplicht (artikel 12, lid 2, WBP) moet ter sprake komen in verband met de eigen integriteit van de systeembeheerder.

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 met het oog hierop persoonsgegevens te verzamelen. In overleg met de ondernemingsraad moet worden vastgesteld welke doeleinden voor controle van e-mail, social media 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, social media en internetgebruik. 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 de 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 per e-mail met derden te communiceren, kan hij aan een steekproefsgewijze inhoudelijke controle onderworpen worden. De controle 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 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 en social media 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 Jeugdformaat. Ook kunnen uitingen van medewerkers via social media worden gerelateerd aan Jeugdformaat. Bij emailgebruik verdient het de voorkeur de controle 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 en social media kan eenvoudig seksuele intimidatie worden gepleegd. Uitlatingen via social media en zowel de inhoud van een e-mailbericht als de bijlagen kunnen seksueel intimiderend zijn. Een werkgever die het beleid hiervoor wil handhaven, kan inkomende e-mailberichten onderwerpen aan een geautomatiseerde controle. De tekst van e-mailberichten kan gescand worden op verboden woorden en verdachte berichten kunnen (geautomatiseerd) teruggestuurd 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 de inkomende berichten en de 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. Deze vorm van controle kan beperkt blijven tot het controleren van de verkeersgegevens. Kennisneming van de inhoud van e-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 stellen aan het persoonlijk gebruik van het e-mailsysteem.
Artikel 5
In de gedragscode kunnen gedragsregels worden opgenomen over wat niet toegestaan is bij een verantwoord e-mailgebruik.

Artikel 6
In de gedragscode kunnen gedragsregels worden opgenomen over wat er in de organisatie onder verantwoord internetgebruik wordt verstaan.

Artikel 7
In de gedragscode kunnen regels worden opgenomen over wat niet is toegestaan bij een verantwoord internetgebruik. Een totaal verbod op het internetgebruik voor persoonlijke doeleinden is niet mogelijk.

Artikel 8
Social media is een verzamelnaam voor alle internet-toepassingen waarmee het mogelijk is om informatie met elkaar te delen op een gebruiksvriendelijke en vaak leuke wijze. Het betreft niet alleen informatie in de vorm van tekst (nieuws, artikelen). Ook geluid (podcasts, muziek) en beeld (fotografie, video) worden gedeeld via social media websites. Met andere woorden, social media staat voor 'Media die je laten socialiseren met de omgeving waarin je je bevindt'. Moderne communicatie draait steeds meer om social media. Twitter, Facebook, Google+, YouTube, LinkedIn, Whatsapp, Snapchat, Instagram, WeChat, Tumblr, Pinterest zijn niet meer weg te denken naast weblogs en andere online communicatie-uitingen. Social media zijn bij uitstek geschikt om kennis te delen en doelgroepen te betrekken bij Jeugdformaat als organisatie. Ook Jeugdformaat medewerkers maken gebruik van social media. Daarbij is het belangrijk om een aantal gedragsregels in het oog te houden. In het algemeen geldt: doe online niets wat je offline ook niet zou doen en houd je aan de Nederlandse wet. Als medewerker van Jeugdformaat dien je je verder te houden aan de geheimhoudingsplicht zoals vastgesteld in de ‘gedragscode jeugdformaat’. Bedenk bij het gebruik van social media dat:

- Het gebruik van social media ‘real time’ gebeurt. Een druk op de knop en jouw bericht staat direct online.
- Online informatie misschien wel eeuwig online staat. Het is niet altijd gemakkelijk om informatie naderhand te (laten) verwijderen.
- Sociale omgangsvormen online net zo goed gelden als offline. Respecteer degene tot wie je je richt. De privacy van anderen wordt gerespecteerd.

In de gedragscode kunnen regels worden opgenomen over verantwoord gebruik van social media.

Artikel 9
Uitleg bij 9.1
Jeugdformaat verwerkt persoonsgegevens van cliënten. De bescherming van de privacy van die cliënten is in verschillende wetten en verdragen geregeld. De belangrijkste wet op dit gebied is de Wet Bescherming Persoonsgegevens (Wbp). De Wbp bevat regels voor het verwerken van persoonsgegevens, het verstrekken of uitwisselen van persoonsgegevens via social media is ook een vorm van verwerking. Bij gebruik van social media kan echter niet worden uitgesloten dat onbevoegden inzage krijgen in persoonsgegevens van de cliënt of de communicatie tussen hulpverlener en cliënt. Zo verzamelen social media aanbieders persoonsgegevens en geven deze door aan derden voor commerciële doeleinden. Voor andere social media geldt dat door de hoge mate van openbaarheid, iedereen kan meelezen, en dat het bereik gigantisch is. Bij het communiceren met of over cliënten via social media is daarom terughoudendheid bij het uitwisselen van persoonsgegevens geboden.

In de gedragscode kunnen regels worden opgenomen over wat niet is toegestaan bij een verantwoord social media gebruik.

Artikel 10
Een werkgever die personeel wil controleren, moet voldoen aan de eisen uit onder meer de Wet bescherming persoonsgegevens (Wbp). De belangrijkste voorwaarden voor de controle van personeel zijn:

- De werkgever heeft een legitieme reden (het zogeheten gerechtvaardigd belang). Dit belang weegt zwaarder dan het privacybelang van het personeel.
- Er zijn geen andere manieren mogelijk om het doel te bereiken, die minder ingrijpend zijn voor de privacy van de werknemers.
- De werkgever meldt de controle bij de Autoriteit Persoonsgegevens.
- De werkgever informeert de werknemers over wat toegestaan en wat verboden is, dat controle mogelijk is en op welke manier dat gebeurt. Dit kan bijvoorbeeld met gedragsregels of een protocol.
- De werkgever houdt rekening met het recht op vertrouwelijke communicatie van de werknemers. Bijvoorbeeld bij de controle van e-mail of telefoon.
- De werkgever vraagt vooraf instemming aan de ondernemingsraad voor de controle.

Voor de heimelijke controle van personeel gelden, naast de voorwaarden voor de ‘gewone’ controle, de volgende extra voorwaarden:

- De werkgever heeft een redelijke verdenking dat een of meerdere medewerkers iets doen wat strafbaar of verboden is.
- De werkgever vraagt bij het de Autoriteit Persoonsgegevens een zogeheten voorafgaand onderzoek aan. De Autoriteit Persoonsgegevens controleert dan of de voorgenomen heimelijke controle is toegestaan. De werkgever mag pas beginnen met de controle als de Autoriteit Persoonsgegevens die heeft goedgekeurd.
- De werkgever informeert de betrokken personeelsleden achteraf altijd over de heimelijke controle. Ook als de controle niet heeft uitgewezen dat de verdenking terecht was.

Uitleg bij 10.7
In eerste instantie vindt alleen controle plaats op basis van getotaliseerde gegevens die niet herleidbaar zijn tot identificeerbare personen. De controle zal (tijdelijk) gerichter worden, zodra een werknemer (of werknemers) ervan verdacht worden de regels te overtreden. Wanneer de werkgever constateert dat een werknemer zich schuldig maakt aan verboden gebruik van e-mail- social media en/of internet, bespreekt hij dit onmiddellijk met de betrokken werknemer. Daarbij wordt de werknemer gewaarschuwd voor de (rechtspositionele) consequenties die het verboden gebruik van e-mail, social media en/of internet voor hem/haar kan hebben.

Uitleg bij 10.8
E-mailberichten van leden van de ondernemingsraad en bedrijfsartsen mogen niet worden gecontroleerd. Dit geldt eveneens voor andere in de onderneming werkzame personen die op grond van hun functie op enige vertrouwelijkheid moeten kunnen beroepen. Voorbeelden hiervan zijn leden van een personeelsvertegenwoordiging, vertrouwenspersonen, leden van een (interne) klachtencommissie etc.

Artikel 11
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/haar betreffende persoonsgegevens worden verwerkt. De werkgever deelt de betrokkene schriftelijk binnen vier weken mee of hem/haar betreffende persoonsgegevens worden verwerkt. De betrokken werknemer kan de werkgever verzoeken de hem/haar 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.