Gedragscode ICT Kindante

Versie 1: 2013

Versie 2: november 2016 (Claudia) kleine aanpassingen m.n. inhoud die niet meer relevant is.

Versie 3: augustus 2017; update met verwijderen inhoud die niet meer van toepassing is en aanvulling social media (vastgesteld door CvB)

Inhoud

Inleiding

De gedragscode ICT van Kindante is een document dat geldt voor iedere medewerker van Kindante. In dit document wordt helder uiteengezet hoe er, in welke situatie, door medewerkers omgegaan dient te worden met:

- Het gebruik van e-mail en internet binnen het netwerk van Kindante
- Het gebruik van vaste telefonie binnen Kindante
- Het gebruik van mobiele (smart)telefonie binnen Kindante en andere mobiele apparaten
- Data (bestanden) die ontsloten worden binnen het netwerk van Kindante

Ook wordt beschreven hoe er, in welke situatie, beveiligingscontroles kunnen worden uitgevoerd op bovenstaand gebruik.
Deze gedragscode geldt voor iedereen die gebruik maakt van het netwerk van Kindante en/of zich in een Kindanteschool bevindt. In deze gedragscode wordt onder “medewerkers’ verstaan:

- Medewerkers met een arbeidsovereenkomst
- Stagiaires
- Uitzend – en freelancekrachten
- Vrijwilligers
- Ouders
- Leerlingen
- Externen

Uitgangspunt is dat iedere medewerker van Kindante de gelegenheid krijgt kennis te nemen van betreffende gedragscode. In de maatschappij zien we in toenemende mate het gebruik van:

- Smarttelefoons en tablets (met internettoegang) door kinderen en personeel op basisscholen
- Sms services, WhatsApp, berichten via social media
- Een fotocamera en/of videocamera op mobiele telefoonapparatuur
- Publiceren van filmpjes en fotomateriaal op vrij toegankelijke internetsites (You-Tube);
- Downloads (Lime Wire, Torrentz)
- Opslagcapaciteit en toenemend gebruik van mobiele gegevensdragers (memorysticks, externe harde schijven, Mp3-spelers, tablets, smartphones)
- Social Media zoals Facebook, LinkedIn, Twitter, Snapchat
- Chatomgevingen (Skype)

Duidelijkheid over wat mag en kan bij betreffende maatschappelijke ontwikkelingen is een vereiste om op een goede wijze om te gaan met deze voorzieningen.

Doel van deze gedragscode is:

- Handhaving van goede naam en integriteit
- Uitdragen van goede waarden en normen
- Tegengaan van “ongewenst gebruik”, seksuele intimidatie, discriminatie of ander onacceptabel gebruik
- Het in bescherming nemen van gebruikers
- Systeem en netwerkbeveiliging
- Kostenbeheersing

Kindante verwacht van medewerkers op het netwerk dat zij rekening houden met het voorgaande en daarom zorgvuldig omgaan met het ICT-netwerken van alle genoemde voorzieningen op de school en op de werkplek.

Als hoofdregel voor dagelijks gebruik geldt dan ook: gebruik de computer en de (mobiele) telefoon en/of voorzieningen in principe voor het werk en/of voor onderwijsdoeleinden. Ieder gebruik in strijd met het doel van deze gedragscode is niet toegestaan.

1. Privacy

Kindante hecht waarde aan privacy van medewerkers en kinderen. De Wet Bescherming Persoonsgegevens staat toe dat de werkgever controleert op onjuist gebruik dan wel misbruik van bedoelde voorzieningen. Deze controlemogelijkheden staan beschreven in deze gedragscode en geven aan op welke wijze en in welke situaties Kindante tot controle kan overgaan. Daarbij is het streven gericht op een goede balans tussen controle en privacybescherming.

2. Beheer

Het Kindantenetwerk wordt in eerste lijn “onderhouden” door de ICT-er op school. Het betreft hier op zeer kleine schaal het kunnen uitvoeren van handelingen, die voor het dagelijks gebruik noodzakelijk zijn. Op hoofdlijnen geschiedt alle onderhoud door Unilogic.
Indien er in deze gedragscode gesproken wordt over de netwerkbeheerder, dan wordt Unilogic Networks bedoeld. In alle andere gevallen wordt “de ICT-er op school” als terminologie gebruikt.

3. Algemene Uitgangspunten

Ieder computernetwerk kent een eigen vorm van kwetsbaarheid en beveiliging. In dit verband worden de gebruikers gewezen op het volgende:

- User-identificatie (inlognaam en wachtwoord) voor het netwerk, maar ook alle softwarepakketten waarvoor moet worden ingelogd, zijn persoonsgebonden en mogen niet aan derden worden doorgegeven.
- Het wordt aanbevolen om wachtwoorden elke drie maanden te veranderen.
- De inhoud en het onderhoud van de home-directory (het aan de gebruiker beschikbaar gestelde deel van de server) valt volledig onder de verantwoordelijkheid van de gebruiker, die deze voorziening zakelijk gebruikt en niet onnodig vult met ‘grote’ bestanden.
- Het up – en downloaden van niet aan onderwijs gerelateerde bestanden is niet toegestaan zonder uitdrukkelijke permissie van de netwerkbeheerder/ICT-er op school. Hier wordt dus niet het up – of downloaden van bestanden t.b.v. de intranetomgeving bedoeld.
- Een systeem waarop de gebruiker heeft ingelogd moet worden afgesloten op het einde van het gebruik; een systeem waarop is ingelogd mag door de gebruiker niet onbewaakt worden achtergelaten. Bij het verlaten van werkplek , wordt m.b.v. sneltoets combinatie windowstoets - L, de toegang tot het netwerk vergrendeld. Op het bestuursbureau worden pc’s na 10 minuten inactiviteit automatisch vergrendeld.
- Iedere gebruiker dient de aanwijzingen van de netwerkbeheerder/ICT-er op school in kwestie op te volgen.
- Bij constatering van storingen en/of andere onregelmatigheden aan computers of het netwerk, inbreuken op beveiliging etc. dient de gebruiker dit terstond aan de netwerkbeheerder of ICT-er van de school te melden.

Het is verboden voor een gebruiker om:

- Zelf software te installeren zonder toestemming van de netwerkbeheerder/ICT-er op school;
- Niet geautoriseerde apparatuur aan te sluiten op het computernetwerk;
- Virussen te maken en/of te verspreiden. Hoewel het hele netwerk uiteraard is beveiligd d.m.v. anti-virusprogrammatuur en firewalls, is de kans aanwezig dat een flexibel ingezet werkstation (b.v. een laptop) , niet is voorzien van de laatste updates. In dat geval is het verplicht om eerst het antivirusprogramma te updaten en dan pas gebruik te maken van een in te pluggen gegevensdrager (b.v. usb-stick), om zo het netwerk niet te vervuilen met virussen, die b.v. van thuis zijn "meegenomen";
- Het computernetwerk te gebruiken om toegang te krijgen tot gegevens die niet voor de gebruiker bestemd zijn, dan wel ander strafbaar gedrag. Dit geldt in de regel ook voor beheerders van het netwerk, ICT-ers op school, of anderen die als beheerder mogen inloggen;
- Opgeslagen bestanden op mobiele gegevensdragers (usb-sticks) die privacygevoelige informatie bevatten, onbeheerd achter te laten, of niet goed genoeg te beschermen tegen verlies of diefstal;
- Storingen of andere onregelmatigheden aan de computers of het netwerk zelf te verhelpen;
- Of op andere wijze te handelen, in strijd met het doel van deze gedragscode.

NB: het gebruik van memorysticks/usb-sticks wordt uit oogpunt van veiligheid afgeraden (i.v.m. verlies/diefstal en eventuele virusoverdracht). Alle data op het netwerk worden bij Unilogic opgeslagen en veilig geback-upt. Deze data en Outlook zijn benaderbaar via het extern bureaublad. Gebruikers worden aangeraden om het extern bureaublad te gebruiken zodat op een andere locatie veilig gewerkt kan worden.

4. Gebruik van Internet

- Gebruikers mogen via het netwerk van Kindante gebruik maken van internet in het kader van de functie-uitoefening of onderwijsactiviteit;
- Medewerkers mogen incidenteel en kortstondig internet gebruiken voor persoonlijke doeleinden, mits dit geen storende onderbreking vormt van de werkzaamheden;
- Het is verboden om auteursrechtelijk beschermde afbeeldingen (gedownload van internet) te verspreiden via bv websites, in nieuwsbrieven of e-mails. Bij schending van auteursrechten is er kans op een boete;
- Het is voor gebruikers verboden middels het netwerk van Kindante internet te gebruiken om:
    - ✓ Te winkelen voor een niet zakelijk doel
    - ✓ Te gokken of deel te nemen aan kansspelen
    - ✓ Niet zakelijke nieuwsgroepen of chatboxen te bezoeken
    - ✓ Websites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten en/of dit materiaal te bekijken of te downloaden
    - ✓ Aanstootgevende informatie waartoe men via internet toegang heeft verkregen zonder toestemming te downloaden, te veranderen, te verspreiden of te vernietigen
    - ✓ Afbeeldingen en videocommunities te bezoeken, die privé-materiaal van wereldburgers publiceert (b.v. You-Tube)
    - ✓ Te mailen met e-mailaccounts anders dan het account van Kindante (Hotmail, Gmail, @Home etc.) en/of het Skype mailadres te gebruiken
    - ✓ Social Media te gebruiken (zoals b.v. Twitter, Facebook, Instagram)

tenzij een van de bovengenoemde zaken een educatief doel dient, of rechtstreeks voortvloeit uit werkzaamheden, die met de functie op school te maken hebben, dan wel met permissie van de direct leidinggevende in kwestie.

5. Gebruik van e-mail

- Iedere medewerker van Kindante kan beschikken over een persoonlijk e-mailadres (leerlingen evt. vanaf groep 5) , om e-mails te ontvangen en te versturen;
- Volwassen gebruikers mogen incidenteel en kortstondig het e-mailsysteem gebruiken voor het ontvangen en versturen van persoonlijke e-mail mits dit geen onderbreking vormt van de werkzaamheden;
- Het versturen van e-mail moet te allen tijde voldoen aan de volgende voorwaarden: correct taalgebruik en een correcte vermelding van de afzender, een duidelijke en ter zake doende inhoud en een eventueel meegestuurde bijlage met een maximale omvang van 3 MB;
- Het is voor gebruikers in ieder geval verboden middels het netwerk van Kindante de e-mailfaciliteit te gebruiken om:
    - ✓ Berichten anoniem of onder een fictieve naam te versturen;
    - ✓ Dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende berichten te versturen. Indien een gebruiker ongevraagd informatie van deze aard krijgt aangeboden, dient dit te worden gemeld aan de netwerkbeheerder, ICT-er op school of aan de directie van de school;
    - ✓ Kettingmailberichten te versturen;
    - ✓ Niet-zakelijke privé-berichten, publicaties/rondschrijven, nieuwsbrieven, reclame, power points e.d. (evt. van buiten de organisatie) te versturen;
    - ✓ Iemand elektronisch lastig te vallen (de ontvanger wenst van de verzender geen mail te ontvangen);
    - ✓ Op andere wijze te handelen in strijd met het doel van deze gedragscode.
- De gebruiker is verplicht zijn e-mailbox regelmatig op te schonen, door niet relevante e-mails met evt. bijlagen te verwijderen uit “postvak-in”, “verzonden items” en “verwijderde items”, teneinde de schijf/opslagcapaciteit niet te overbelasten. Met de intrede van digitale fotografie en de scanfaciliteit van onze multifunctionals neemt het aantal bestanden, ook in mailboxen, soms extreem toe. Het is de verantwoordelijkheid van iedere gebruiker van het Kindantenetwerk, om zo effectief mogelijk om te gaan met de beschikbare schijfruimte.

6. Het gebruik van vaste telefoon

- Medewerkers van Kindante mogen telefoons van Kindante gebruiken in het kader van functie-uitoefening;
- Medewerkers mogen incidenteel en kortstondig de telefoon gebruiken voor het voeren van privégesprekken als daar uit noodzaak aanleiding toe is, mits dit geen storende onderbreking vormt van de werkzaamheden;
- Het is in ieder geval voor gebruikers verboden telefoons van Kindante te gebruiken om:
    - ✓ Service- en amusementsnummers te bellen die beginnen met 0906 en 0909, tenzij dit gebeurt vanuit een schoolse aangelegenheid;
    - ✓ Internationale nummers te bellen voor privédoeleinden.

7. Gebruik van zakelijk ter beschikking gestelde mobiele telefoon (GSM) c.q. abonnement

- De zakelijk ter beschikking gestelde mobiele telefoon c.q. het abonnement wordt ingezet, of beschikbaar gesteld, om de mobiele bereikbaarheid van een medewerker te realiseren en dient overwegend voor inkomende telefoongesprekken en berichten;
- Iedereen die een zakelijke mobiele telefoon c.q. het abonnement gebruikt, dient terughoudend om te gaan met het voeren van uitgaande telefoongesprekken en berichten via de mobiele telefoon, tenzij dat uit hoofde van de functie noodzakelijk is;
- Bij uitgaande gesprekken en berichten dient dan ook het urgente zakelijke karakter voorop te staan en geniet het gebruik van een vaste (VoIP) telefoon altijd de voorkeur;
- Het is een medewerker toegestaan om een ter beschikking gestelde mobiele telefoon c.q. het abonnement te gebruiken om te telefoneren of te smssen, te pingen, WhatsApp te gebruiken, te fotograferen, te filmen, geluidsfragmenten op te nemen, of te surfen op internet, als daar werk gerelateerd behoefte aan is;
- De kosten van het gebruik van een mobiele telefoon van Kindante in het buitenland worden bij de gebruiker in rekening gebracht, tenzij er sprake is van een aantoonbare dienstreis en de kosten voortkomen uit zakelijke gesprekken.

8. Gebruik van mobiele telefoons door leerlingen of ouders

- A. Een mobiele telefoon van een leerling mag onder schooltijd niet gebruikt worden, tenzij dit een onderwijskundig doel dient en geautoriseerd is door de directie van school;
- B. Het niet gebruiken van een mobiele telefoon impliceert dus ook het verbod op opnemen van geluidsfragmenten, het nemen van foto's of het maken van video-opnames binnen school (ook voor ouders!), tenzij daarvoor toestemming is gegeven door de directie;
- C. Zijn er al met toestemming bestanden zoals genoemd in 8B gemaakt, dan is het publiceren van deze bestanden middels internet of e-mail ten strengste verboden, tenzij daar door alle personen, voorkomend op die bestanden, toestemming voor is verleend.

9. Monitoring VoIP – telefoonverkeer

- A. Monitoring van telefoongebruik vindt slechts plaats in het kader van de doelstelling van de gedragscode, zoals in de inleiding verwoord;
- B. Het genereren van gegevens uit de VoIP - centrale vindt in beginsel plaats op het niveau van de Kindanteorganisatie en wordt een-op-een gecommuniceerd op schoolniveau; praktisch gezien, worden de gegenereerde gegevens automatisch, per mail, Pdf-formaat doorgezet naar de betreffende directie van een VoIP school met een maandelijkse frequentie;
- C. De gegenereerde gegevens van VoIP verschaffen inzicht in verkeersgegevens, nooit op inhoud;
- D. Met verkeersgegevens wordt bedoeld: per toestelnummer kan inzichtelijk worden gemaakt: het aantal uitgaande gesprekken en totale gespreksduur per toestel per maand;
- E. Ontvangen gesprekken op een toestelnummer zijn niet te monitoren;
- F. De directies, waarvan de scholen zijn aangesloten op het (VoIP) telefoonnetwerk, ontvangen maandelijks de gegenereerde gegevens zoals genoemd onder D).Het betreft hier een overzicht van het aantal gevoerde gesprekken per toestel in de schoolorganisatie en de totale gespreksduur; pas bij verdenking van zwaar misbruik, b.v. zeer hoge belkosten of extreem veel telefoonverkeer, kan er op verzoek een overzicht worden gegenereerd waarop niet alleen het aantal gesprekken per toestel wordt getoond, maar ook de nummers waar naartoe werd gebeld.

10. Monitoring e-mailverkeer

- Monitoring van e-mailverkeer vindt slechts plaats in het kader van de doelstelling van de gedragscode, zoals in de inleiding verwoord;
- De netwerkbeheerder/ICT-er op school kan de postbusgroottes van gebruikers in gebruikersstatistieken genereren, om tijdig te kunnen sturen op de capaciteit van schijfruimte;
- Bij de monitoring van e-mail, gaat het over aantallen mails in postvak-in, verzonden items en verwijderde items, of de totale bestandsgrootte van genoemde boxen, nooit over de inhoud;
- Indien de postbus van een gebruiker de maximale grootte overschrijdt, zal de ICT-er op school, in overleg met de gebruiker trachten de postbus op te schonen, opdat de inhoud van de postbus kan worden teruggebracht naar de toegestane omvang;
- De postbusgrootte kan afhankelijk van de functies van personeelsleden worden aangepast;
- E-mails met attachments, die voor meerdere personen in een organisatie tegelijk worden verstuurd geldt: het attachment, een bestand, wordt in het netwerk maar 1 keer centraal opgeslagen, om overvolle dataschijven en mappen van gebruikers te voorkomen; het geniet te allen tijde de voorkeur, om bestanden van deze aard te delen op de dataschijf , dan wel op Intranet-omgeving (Boekenkast Afas).

11. Monitoring van internetverkeer

- Monitoring van internetverkeer vindt slechts plaats in het kader van de doelstelling van de gedragscode, door Unilogic Networks, zoals in de inleiding verwoord;
- Internetverkeer wordt uit oogpunt van overdrachtssnelheden continu gemonitord door de netwerkbeheerder Unilogic Networks, in het kader van performance-checks;
- Misbruik van internet kan getraceerd worden als een werkstation in het gehele Kindantenetwerk zorg draagt voor een red alert, dat veroorzaakt wordt door enorm datatransport tussen het netwerkstation en het World Wide Web. Dergelijk misbruik wordt in eerste instantie opgemerkt door Unilogic Networks en gecommuniceerd met de senior adviseur onderwijs/ICT van de stichting, die dit oppakt met de leidinggevende van de desbetreffende Kindantelocatie;
- Bij de monitoring van misbruik van internet, kan worden nagegaan welke gebruiker wanneer op welk netwerkstation van Kindante, welke website bezoekt of heeft bezocht.

12. Mobiele telefonie, e-mailverkeer en internetgedrag, werk-gerelateerd in de privé situatie

Het is vandaag de dag heel gewoon dat werknemers “telewerken”. Hiermee wordt bedoeld dat vanuit de privé-situatie ingelogd kan worden op het netwerk t.b.v. mail en/of het bewerken van bestanden. Bovendien worden steeds meer webapplicaties gebruikt (b.v. Esis, website van school, Intranet). Ook hier gelden de gedragsregels, zoals in deze gedragscode genoemd m.b.t. inhoud, het algemeen gebruik en omgang met inloggegevens zoals gebruikersnaam en wachtwoorden.

Met klem worden alle gebruikers van het netwerk van Kindante erop geattendeerd, om juist in de thuissituatie of op een andere werkplek buiten school of kantoor zeer voorzichtig om te gaan met inloggegevens en wachtwoorden en nooit de p.c. of laptop onbeheerd achter te laten zonder uit te loggen. Denk hierbij aan uw eigen privacygevoelige informatie, die van Kindante en/of die van collega’s, kinderen en ouders. Ook hier geldt het advies om wachtwoorden iedere drie maanden te veranderen.

13. Richtlijnen voor het gebruik van Social Media

Social media zijn niet meer weg te denken uit de manier waarop we vandaag de dag communiceren. Social media zijn zeer geschikt om in te zetten voor communicatie met de verschillende doelgroepen waar we mee werken. Van belang is te beseffen dat je met berichten op social media (onbewust) de goede naam van een school of Kindante en betrokkenen ook kunt schaden. Om deze reden verwacht Kindante dat alle medewerkers bewust met social media omgaan. In dit document staan de belangrijkste richtlijnen voor het gebruik van social media genoemd.

- De school zorgt ook digitaal voor een veilig klimaat en communiceert met medewerkers, leerlingen en ouders hoe zij dit doet.
- Stem vooraf af of de pagina openbaar wordt of enkel bestemd is voor een besloten groep.
- Bedenk dat bij een openbare pagina, geplaatste berichten (en foto's) door alle volgers gedeeld kunnen worden en dus openbaar worden en zichtbaar voor iedereen.
- Check voor het plaatsen van foto's en/of namen van leerlingen en medewerkers of zij hier toestemming voor hebben gegeven.
- Plaats bij de foto's geen namen. Niemand wordt dan in verlegenheid gebracht door de foto's.
- De school deelt kennis en andere waardevolle informatie, zoals nieuwe ontwikkelingen binnen school of Kindante.
- Let op het taalgebruik: vermijd taalfouten, onduidelijke zinnen of woorden. o Realiseer dat internetberichten blijvend zijn.
- Indien negatieve berichten of reacties op de social media-pagina van de school worden geschreven: geef er niet impulsief een reactie op. Ga er met de betrokkenen over in een persoonlijk gesprek. o De school behoudt het recht om ongepaste reacties (bijvoorbeeld ongepast taalgebruik) te verwijderen.
- Negatieve reacties worden niet uit de weg gegaan, als ze maar opbouwend bedoeld zijn.
- Deel geen vertrouwelijke informatie over de school of over Kindante.
- Schrijf nooit een negatief bericht of reactie over een andere school, organisatie of over medewerkers/leerlingen/ouders/partners.
- Schrijf geen negatieve berichten/oordelen over de school, Kindante of bijvoorbeeld wetsvoorstellen.
- Zet geen persoonlijke berichten (bijvoorbeeld over je familie of vrienden) op de social mediapagina van de school.
- Reageer niet vanuit de schoolpagina op berichten van vrienden. Houd werk en privé gescheiden! o Maak geen gebruik van de mogelijkheid 'pagina promoten'; dit kost geld!

Social media hebben soms als gevolg dat er een grijs gebied ontstaat tussen je persoonlijke leven en werk. Uitgangspunt is dat professionals zelf weten hoe zij hiermee verstandig omgaan.
Hoofdregel: het gedrag van leraren op social media wijkt niet af van wat in de klas of op school gebruikelijk is. Kindante respecteert de vrijheid van meningsuiting van haar medewerkers, maar herinnert je eraan dat je als medewerker een voorbeeldfunctie hebt en altijd ambassadeur van Kindante bent. Je mag werk gerelateerde onderwerpen publiceren mits het geen vertrouwelijke informatie over Kindante betreft. De publicatie mag Kindante niet schaden. Bij twijfel niet publiceren, of ga in overleg met je leidinggevende of de communicatieadviseur.

Laat als ambassadeur van Kindante en van de school vooral de goede, positieve kanten van je werk zien via social media.
Indien je negatieve of positieve berichten over een school van Kindante of Kindante signaleert, stuur deze dan naar de communicatieadviseur Maud Golsteyn (m.golsteyn@kindante.nl) en je leidinggevende. Vermijd de verleiding om impulsief te reageren (bijvoorbeeld omdat je emotioneel betrokken bent). Stem bij twijfel altijd af met de communicatieadviseur en je leidinggevende.

Je bent op de hoogte dat publicaties op social media altijd vindbaar zijn en vaak vindbaar blijven.
Bij onderwijsinhoudelijke onderwerpen maak je duidelijk dat je op persoonlijke titel publiceert.

Plaats, deel of like nooit vertrouwelijke informatie over de school of over Kindante op social media.
Plaats, deel of like geen berichten die tegenstrijdig zijn met beleid van de school of van Kindante, of berichten die schadelijk kunnen zijn voor de school of Kindante.

Ben voorzichtig in de digitale omgang met leerlingen en ouders op social media.
Plaats geen foto's/ informatie van/over leerlingen op je eigen social media.
Ga niet in discussie met een leerling of ouder op social media. In het geval dat een discussie dreigt te ontsporen, neem dan direct contact op met de leidinggevende om de te volgen strategie te bepalen.

Als je LinkedIn-, Twitter-, Instagram- of Facebookpagina openbaar is, kan je toekomstig werkgever deze bekijken. Sterker nog, volgens het College Bescherming Persoonsgegevens (CBP) hebben werkgevers daar alle recht toe aangezien de informatie via social media en Google openbaar is. Gebruik maken van deze informatie in het gesprek zonder dat te vermelden is niet netjes, maar mogelijk.

Houd rekening met het wettelijk vastgelegde auteurs-, beeld- en citaatrecht. Het is verboden om zonder toestemming van de maker andermans werk te publiceren. Schending van deze wet levert je een boete op van honderden euro's.

Kindante mag een medewerker aanspreken als zijn of haar uitingen op social media niet geoorloofd of gepast zijn. Bij grove schendingen van de code kan tevens een gesteld disfunctioneren of ontslag onderbouwd worden.