



Internet- en e-mailgebruik

Datum opmaak : 1 december 2008

Datum inwerkingtreding : 15 mei 2009

Procedurenummer : 08-002

Het Reynaertcollege gevestigd te Hulst

Gelet op

- Artikel 125ter Ambtenarenwet/ artikel 7:611 BW;
- De Wet Bescherming Persoonsgegevens (WBP);
- Artikel 12 lid 1 sub m en n en 14 lid 3 d Wet Medezeggenschap Scholen

Overwegende dat

- Het Reynaertcollege en haar werknemers zich ten opzichte van elkaar dienen te gedragen als goed werkgever en goed werknemer;
- Het Reynaertcollege en haar leerlingen zich ten opzichte van elkaar met respect dienen te gedragen;
- het internet- en e-mailgebruik voor (veel van) de werknemers en leerlingen noodzakelijk is om hun werk/ studie 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 en leerlingen verantwoord gebruik van internet en e-mail wordt verwacht;
- het Reynaertcollege 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 school;
- de onderhavige gedragscode voorschriften en maatregelen bevat zoals hiervoor genoemd;
- het Reynaertcollege gerechtigd is persoonsgegevens te verwerken ten behoeve van de controle op de naleving van deze gedragscode;
- het Reynaertcollege bij de controle van de naleving de fundamentele rechten en vrijheden van de betrokken werknemer(s) en leerling(en) in acht neemt, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer (artikel 8 sub f WBP).

Heeft het Reynaertcollege, met instemming van de MR de navolgende gedragscode vastgesteld:

Regeling internet en e-mail gebruik

1. Begripsbepalingen/ werkingssfeer

Deze regeling is van toepassing op alle geheel of gedeeltelijk geautomatiseerde verwerkingen van persoonsgegevens van personen in dienst van of werkzaam voor het Reynaertcollege Hulst.

Verantwoordelijke : het Bestuur van het Reynaertcollege.
Leidinggevende : het verantwoordelijke lid van het Managementteam

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).
- 2.2 De controle op e-mail- en internetgebruik binnen het Reynaertcollege zal conform deze regeling worden uitgevoerd. Indien er zich situaties voordoen waarin deze regeling niet voorziet, zal conform het wettelijke kader en de WBP en in overleg met de PMR 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 zes maanden.
- 2.5 De Directie 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 en internetgebruik en regels over de wijze waarop controle op persoonsgegevens over e-mail- en internetgebruik plaats vindt.
- 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 vertrouwelijke gegevens c.q. informatie
 - d. Systeem en netwerkbeveiliging
 - e. Capaciteitsbeheersing
 - f. Tegengaan van discriminatie
 - g. Tegengaan verboden gebruik

4. E-mailgebruik en internetgebruik

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

- 4.2 De medewerker maakt uit hoofde van zijn functie enkel gebruik van het door het Reynaertcollege verstrekte e-mailadres.
- 4.3 Het versturen van e-mail berichten moet voldoen aan de volgende voorwaarden:
- aan de mail zal automatisch een disclaimer worden toegevoegd;
 - houd de mail kort, zakelijk en respectvol. Hierbij gelden de normale gedragsregels;
 - beoordeel bij het doorsturen van een mail of het nodig is de voorgaande informatie integraal door te sturen;
 - voer geen discussie via de mail;
 - er wordt een correcte melding van de afzender gegeven.
- 4.4 Beperkt persoonlijk gebruik van het e-mail- en internetsysteem is evenwel toegestaan, mits dit niet storend voor de dagelijkse werkzaamheden is, het computernetwerk hierdoor niet onnodig wordt belast en dit geen verboden gebruik in de zin van artikel 5 oplevert.
- 4.5 Bijlage(n) bij een e-mail waarvan de afzender onbekend is, worden in verband met het risico op virussen niet geopend en door de ontvanger direct verwijderd.
- 4.6 De werknemer zal diens persoonsgebonden gebruikersnaam en wachtwoorden aan niemand bekend maken. Hij/ zij blijft verantwoordelijk voor alle acties die met behulp van zijn/ haar gebruikersnaam worden uitgevoerd, tenzij hij/ zij het tegendeel kan bewijzen.
- 4.7 Om de continuïteit van de werkzaamheden te waarborgen, kan de leidinggevende bij langdurige afwezigheid van de medewerker via de Systeembeheerder toegang krijgen tot het e-mailverkeer van de medewerker. De Systeembeheerder doet hiervan jaarlijks verslag aan het Managementteam.
- 4.8 De medewerker verplicht zich de computer waarop is gewerkt, dan wel deze tijdelijk verlaat, te locken of af te sluiten teneinde ongeautoriseerd gebruik te voorkomen.
- 4.9 Verboden e-mail en internetgebruik wordt zo veel mogelijk softwarematig onmogelijk gemaakt.

5. Verboden e-mail- en internetgebruik

- 5.1 Het is de werknemer niet toegestaan om het e-mailsysteem te gebruiken voor het verzenden van:
- berichten met een pornografische, racistische, discriminerende, beledigende of aanstootgevende inhoud;
 - kettingbrieven en reclame;
 - berichten met een (seksueel) intimiderende en/ of dreigende inhoud;
 - berichten die (kunnen) aanzetten tot haat en/ of geweld;
 - anonieme berichten of berichten onder een fictieve naam.
- 5.2 Het is de medewerker niet toegestaan om ongeoorloofd en/ of onrechtmatig in andermans bestanden rond te kijken, deze te wijzigen, te gebruiken of te verwijderen. Ook pogingen daartoe zijn niet toegestaan.

- 5.3 Het is de werknemer niet toegestaan om op internet sites te bezoeken die:
- in strijd zijn met de wet;
 - bijv. pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten. Noch is het toegestaan dergelijk materiaal te downloaden.
 - (gok)spelletjes, koopwaar, kansspelen, chat-/ babbelboxen aanbieden, tenzij zulks past in het kader van de onderwijsactiviteiten.
- 5.4 Het is de werknemer niet toegestaan om zich ongeoorloofd toegang tot niet openbare bronnen op internet te verschaffen.
- 5.5 Het is de werknemer, met uitzondering van de Systeembeheerder, niet toegestaan om software en applicaties te downloaden.
- 5.6 Het is de medewerker niet toegestaan om in de e-mail of op het internet in strijd met de wet of onethisch te handelen.

6. Voorwaarden voor controle

- 6.1 Controle van persoonsgegevens over e-mail- en internetgebruik vindt slechts plaats in het kader van in artikel 3.2 genoemde doelen.
- 6.2 Controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot identificeerbare persoon.
- 6.3 Indien een werknemer of een groep werknemers wordt verdacht de regels te overtreden, kan gedurende een vastgestelde (korte) periode gerichte controle plaats vinden.
- 6.4 Controle beperkt zich in beginsel tot verkeersgegevens van het e-mail- en internetgebruik slechts bij zwaarwegende redenen vindt controle op de inhoud plaats. Dit ter beoordeling aan de Directie.
- 6.5 E-mail berichten van leden van de medezeggenschapsraad onderling, van bedrijfsartsen, verzuimconsulenten, directieleden en P&O-medewerkers worden uitgesloten van controle. De uitsluiting geldt niet voor de controle op de veiligheid van het berichtenverkeer.

7. Controle

- 7.1 De controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot individuele personen. Indien een medewerker of een groep medewerkers ervan verdacht wordt de regels te overtreden, kan gedurende een vastgestelde (korte) periode gerichte controle plaats vinden
- 7.2 Het Reynaertcollege zal niet de inhoud van zowel persoonlijke als zakelijke e-mailberichten lezen. Eveneens zullen persoonsgegevens omtrent het aantal mails, de mail-adressen en andere data hieromtrent niet geregistreerd en/ of gecontroleerd worden. Dit laat onverlet dat controles op incidentele basis vanwege een zwaarwichtige reden kunnen plaats vinden, uitgezonderd het bepaalde in artikel 6.5 van dit reglement.

- 7.3 De controle ter voorkoming van negatieve publiciteit en seksuele intimidatie en de controle in het kader van systeem- en netwerkbeveiliging vindt plaats op basis van content-filtering. Verdachte berichten worden automatisch teruggestuurd naar de afzender.
- 7.4 De controle in het kader van de capaciteitsbeheersing wordt beperkt tot verkeersgegevens.
- 7.5 Persoonsgegevens over e-mail en internetgebruik worden niet langer bewaard dan noodzakelijk, met een maximum bewaartermijn van zes maanden.
- 7.6 De concretisering van de controle is als volgt te omschrijven. Steekproefsgewijs zal twee maal per schooljaar op een willekeurig tijdstip gedurende één maand een logfile worden bijgehouden van het e-mail- en het internetverkeer. Dit met inachtneming van dit reglement. Vervolgens wordt hier een gedepersonaliseerde rapportage met betrekking tot personen die bestaat uit de volgende onderdelen en met de volgende doelen:

Onderdelen:

1. Geblokkeerde websites
Aantal keer geblokkeerd
Top 20 geblokkeerde sites
2. Top 20 bezochte sites
3. Aantal personen per geblokkeerde website
4. Downloads van verboden bestandstypen
5. Personen meer dan 10 keer geblokkeerd (anoniem)

Doelen:

- Verbetering van het filter
Inzicht in het internetgebruik
- Verbetering van het filter
Inzicht in het internetgebruik
- Inzicht in het internetgebruik
- Systeem- en netwerkbeveiliging
- Het tegengaan van gebruik strijdig met de doelstelling en identiteit van de school

De gedepersonaliseerde rapportage wordt verstrekt aan de Directie en de MR. De Directie kan naar aanleiding van deze rapportage vragen om een gepersonaliseerde rapportage.

8. Sancties

- 8.1 Personeelsleden worden door de Directie over het bestaan van dit reglement op de hoogte gebracht. Nieuwe personeelsleden ontvangen het reglement bij indiensttreding. Zodra de medewerker met het reglement bekend is, is hij/ zij hieraan gebonden.
- 8.2 Wanneer het Reynaertcollege constateert dat een werknemer zich schuldig maakt aan verboden gebruik van het e-mail- en/ of internetsysteem, bespreekt de Directie in aanwezigheid van de Stafmedewerker P&O, 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. Afhankelijk van de aard van het e-mailgebruik of het internetgedrag kan worden overgegaan tot:
- het houden van een gesprek, waarvan het verslag in het personeelsdossier wordt bewaard gedurende een periode van een kalenderjaar;

- het geven van een schriftelijke waarschuwing, die geldt voor de periode van drie kalenderjaren;
- schade kan worden verhaald op de gebruiker;
- andere maatregelen, zoals uitsluiting van toegang tot het systeem. In uitzonderlijke gevallen kan ontslag tot de mogelijkheden behoren.

8.3 Gedrukte en niet gedrukte lograpporten worden gedurende de periode van één jaar bewaard door de Directie en daarna vernietigd.

9. Rechten van de werknemer

- 9.1 De Directie informeert de werknemer 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 (artikel 33 WBP).
- 9.2 De werknemer kan zich tot de Directie wenden met het verzoek voor een volledig overzicht van zijn bewerkte persoonsgegevens. Het verzoek wordt binnen vier weken beantwoord (artikel 35 WBP).
- 9.3 De werknemer kan de Directie 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 vier weken beantwoord (artikel 36 WBP).
- 9.4 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.
- 9.5 De medewerker kan bij de Directie verzet aantekenen tegen de verwerking van diens persoonsgegevens in verband met bijzondere persoonlijke omstandigheden. De Directie oordeelt binnen vier weken na ontvangst van het verzet of dit gerechtvaardigd is. Indien het verzet gerechtvaardigd wordt geacht, wordt de verwerking van de betreffende gegevens terstond beëindigd (artikel 40 WBP).
- 9.6 Indien de medewerker meent benadeeld te zijn in de rechten op grond van dit reglement, kan hij/ zij zich richten tot de Stafmedewerker P&O.

Regeling internet en e-mail gebruik leerlingen (bijlage bij leerlingenstatuut)

1. Begripsbepalingen/ werkingssfeer

Deze regeling is van toepassing op alle geheel of gedeeltelijk geautomatiseerde verwerkingen van persoonsgegevens van leerlingen van het Reynaertcollege Hulst.

Verantwoordelijke : het Bestuur van het Reynaertcollege.
Leidinggevende : het verantwoordelijke lid van het Managementteam

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).
- 2.2 De controle op e-mail- en internetgebruik binnen het Reynaertcollege zal conform deze regeling worden uitgevoerd. Indien er zich situaties voordoen waarin deze regeling niet voorziet, zal conform het wettelijke kader en de WBP en in overleg met de MR gehandeld worden.
- 2.3 Gestreefd wordt naar verantwoord e-mail- en internetgebruik en bescherming van de privacy van leerlingen op de werkplek.
- 2.4 Persoonsgegevens van e-mail en internetgebruik worden niet langer bewaard dan noodzakelijk, met een maximum bewaartermijn van zes maanden.
- 2.5 De Directie 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 en internetgebruik en regels over de wijze waarop controle op persoonsgegevens over e-mail- en internetgebruik plaats vindt.
- 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 vertrouwelijke gegevens c.q. informatie
 - d. Systeem en netwerkbeveiliging
 - e. Capaciteitsbeheersing
 - f. Tegengaan van discriminatie
 - g. Tegengaan verboden gebruik

4. E-mailgebruik en internetgebruik

- 4.1 Het e-mail- en internetsysteem wordt aan de leerling voor zakelijk gebruik beschikbaar gesteld. Gebruik is derhalve verbonden met taken die voortvloeien uit de opdracht.

- 4.2 De leerling maakt geen privégebruik van de op het Reynaertcollege gebruikte ELO (Elektronische leeromgeving).
- 4.3 Het versturen van e-mail berichten moet voldoen aan de volgende voorwaarden:
- aan de mail zal automatisch een disclaimer worden toegevoegd;
 - houd de mail kort, zakelijk en respectvol. Hierbij gelden de normale gedragsregels;
 - beoordeel bij het doorsturen van een mail of het nodig is de voorgaande informatie integraal door te sturen;
 - voer geen discussie via de mail;
 - er wordt een correcte melding van de afzender gegeven.
- 4.4 Bijlage(n) bij een e-mail waarvan de afzender onbekend is, worden in verband met het risico op virussen niet geopend en door de ontvanger direct verwijderd.
- 4.5 De leerling zal diens persoonsgebonden gebruikersnaam en wachtwoorden aan niemand bekend maken. Hij/ zij blijft verantwoordelijk voor alle acties die met behulp van zijn/ haar gebruikersnaam worden uitgevoerd, tenzij hij/ zij het tegendeel kan bewijzen.
- 4.6 Een leidinggevende kan via de systeembeheerder toegang krijgen tot het e-mailverkeer van de leerling.
- 4.7 Verboden e-mail en internetgebruik wordt zo veel mogelijk softwarematig onmogelijk gemaakt.

5. Verboden e-mail- en internetgebruik

- 5.1 Het is de leerling niet toegestaan om het e-mailsysteem te gebruiken voor het verzenden van:
- berichten met een pornografische, racistische, discriminerende, beledigende of aanstootgevende inhoud;
 - kettingbrieven en reclame;
 - berichten met een (seksueel) intimiderende en/ of dreigende inhoud;
 - berichten die (kunnen) aanzetten tot haat en/ of geweld;
 - anonieme berichten of berichten onder een fictieve naam.
- 5.2 Het is de leerling niet toegestaan om ongeoorloofd en/ of onrechtmatig in andermans bestanden rond te kijken, deze te wijzigen, te gebruiken of te verwijderen. Ook pogingen daartoe zijn niet toegestaan.
- 5.3 Het is de leerling niet toegestaan om op internet sites te bezoeken die:
- in strijd zijn met de wet;
 - bijv. pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten. Noch is het toegestaan dergelijk materiaal te downloaden.
 - (gok)spelletjes, koopwaar, kansspelen, chat-/ babbelboxen aanbieden, tenzij zulks past in het kader van de onderwijsactiviteiten.
- 5.4 Het is de leerling niet toegestaan om zich ongeoorloofd toegang tot niet openbare bronnen op internet te verschaffen.

- 5.5 Het is de leerling niet toegestaan om software en applicaties te downloaden.
- 5.6 Het is de leerling niet toegestaan om in de e-mail of op het internet in strijd met de wet of onethisch te handelen.

6. Voorwaarden voor controle

- 6.1 Controle van persoonsgegevens over e-mail- en internetgebruik vindt slechts plaats in het kader van in artikel 3.2 genoemde doelen.
- 6.2 Controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot identificeerbare persoon.
- 6.3 Indien een leerling of een groep leerlingen wordt verdacht de regels te overtreden, kan gedurende een vastgestelde periode uitsluiting van e-mailverkeer en internetgebruik plaatsvinden.

7. Controle

- 7.1 De controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot individuele personen. Indien een leerling of een groep leerlingen ervan verdacht wordt de regels te overtreden, kan gedurende een vastgestelde (korte) periode gerichte controle plaats vinden.
- 7.2 Het Reynaertcollege zal niet de inhoud van zowel persoonlijke als zakelijke e-mailberichten lezen. Eveneens zullen persoonsgegevens omtrent het aantal mails, de mail-adressen en andere data hieromtrent niet geregistreerd en/ of gecontroleerd worden. Dit laat onverlet dat controles op incidentele basis vanwege een zwaarwichtige reden kunnen plaats vinden.
- 7.3 De controle ter voorkoming van negatieve publiciteit en seksuele intimidatie en de controle in het kader van systeem- en netwerkbeveiliging vindt plaats op basis van content-filtering. Verdachte berichten worden automatisch verwijderd/ naar de afzender teruggestuurd.
- 7.4 De controle in het kader van de capaciteitsbeheersing wordt beperkt tot verkeersgegevens.
- 7.5 Persoonsgegevens over e-mail en internetgebruik worden niet langer bewaard dan noodzakelijk, met een maximum bewaartermijn van zes maanden.
- 7.6 De concretisering van de controle is als volgt te omschrijven. Steekproefsgewijs zal twee maal per schooljaar op een willekeurig tijdstip gedurende één maand een logfile worden bijgehouden van het e-mail- en het internetverkeer. Dit met inachtneming van dit reglement. Vervolgens wordt hiervan een gedepersonaliseerde rapportage gemaakt met betrekking tot personen die bestaat uit de volgende onderdelen en met de volgende doelen:

Onderdelen:

1. Geblokkeerde websites
Aantal keer geblokkeerd

Doelen:

Verbetering van het filter

Top 20 geblokkeerde sites	Inzicht in het internetgebruik
2. Top 20 bezochte sites	Verbetering van het filter Inzicht in het internetgebruik
3. Aantal personen per geblokkeerde website	Inzicht in het internetgebruik
4. Downloads van verboden bestandstypen	Systeem- en netwerkbeveiliging
5. Personen meer dan 10 keer geblokkeerd (anoniem)	Het tegengaan van gebruik strijdig met de doelstelling en identiteit van de school

De gedepersonaliseerde rapportage wordt verstrekt aan de Directie en de MR. De Directie kan naar aanleiding van deze rapportage vragen om een gepersonaliseerde rapportage.

8. Sancties

- 8.1 Leerlingen en ouders worden door de mentoren en in de schoolgids op de hoogte gebracht van het bestaan van deze regeling. Voor de volledige tekst verwijzen we naar de website. Zodra de leerling met het reglement bekend is, is hij/ zij hieraan verbonden.
- 8.2 Wanneer het Reynaertcollege constateert dat een leerling zich schuldig maakt aan verboden gebruik van het e-mail- en/ of internetsysteem, bespreekt de Directie in aanwezigheid van de mentor, dit onmiddellijk met de betrokken leerling. Daarbij wordt de leerling gewaarschuwd voor de consequenties die het verboden gebruik van het e-mail en/ of internetsysteem voor hem kan hebben. Afhankelijk van de aard van het e-mailgebruik of het internetgedrag kan worden overgegaan tot:
- het houden van een gesprek, waarvan het verslag in het dossier wordt bewaard;
 - het geven van een schriftelijke waarschuwing naar de ouders/verzorgers toe;
 - schade kan worden verhaald op de gebruiker ;
 - andere maatregelen, zoals uitsluiting van toegang tot het systeem.

9. Rechten van de leerling

- 9.1 De Directie informeert de leerling 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 (artikel 33 WBP).
- 9.2 De leerling kan zich tot de Directie wenden met het verzoek voor een volledig overzicht van zijn bewerkte persoonsgegevens. Het verzoek wordt binnen vier weken beantwoord (artikel 35 WBP).
- 9.3 De leerling kan de Directie 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 vier weken beantwoord (artikel 36 WBP).
- 9.4 Een weigering is met redenen omkleed. De leerling draagt er zorg voor dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd.

- 9.5 De leerling kan bij de Directie verzet aantekenen tegen de verwerking van diens persoonsgegevens in verband met bijzondere persoonlijke omstandigheden. De Directie oordeelt binnen vier weken na ontvangst van het verzet of dit gerechtvaardigd is. Indien het verzet gerechtvaardigd wordt geacht, wordt de verwerking van de betreffende gegevens terstond beëindigd (artikel 40 WBP).
- 9.6 Indien de leerling meent benadeeld te zijn in de rechten op grond van dit reglement, kan hij/ zij zich richten tot de Directie.

Slotbepaling gedragscode internet en e-mail gebruik

- 1 Deze gedragscode kan worden aangehaald als "Regeling Internet- en e-mailgebruik".
- 2 Het Reynaertcollege kan deze gedragscode met instemming van de MR wijzigen of intrekken. De wijzigingen worden schriftelijk vastgelegd en voorafgaand aan de invoering aan de medewerkers bekend gemaakt.
- 3 Deze regeling is tot stand gekomen in overleg en na raadpleging van de MR op 12 maart 2009.

Afdelingsdirecteur a.i.:
De heer W.A.J. Sandtke

Voorzitter MR:
Mevr. M.M.L. Meesen-Sponselee

