

Regeling Elektronische informatie- en communicatiemiddelen (EIC) (onlosmakelijk verbonden met de Gedragscode)	
Werkveld:	Personele Zaken, Onderwijsinnovatie & ICT S.H.W. Kroon/ K. Van den Berg
Datum:	Januari 2017
Versie:	1.0
Vastgesteld bestuur:	
Instemming/Advies GMR:	

Regeling

Elektronische informatie- en communicatiemiddelen (EIC)

Inhoud

Inleiding.....	3
Artikel 1 Doel en werkingssfeer van deze regeling.....	4
Artikel 2 Algemene uitgangspunten	4
Artikel 3 Gebruik van elektronische informatie- en communicatiemiddelen	4
Artikel 4 Meldingsplicht	5
Artikel 5 Controle	5
Artikel 6 Inwerkingtreding en citeertitel.....	6
Toelichting op de EIC- modelregeling	7
Artikelsgewijze toelichting	8
Artikel 1 Doel van deze regeling	8
Artikel 2 Algemene uitgangspunten	8
Artikel 3 Gebruik van elektronische informatie- en communicatiemiddelen	8
Artikel 5 Controle	9

Inleiding

Middels deze regeling geven wij een praktische vertaling van de diverse wetgeving¹ op het gebied van bescherming Persoonsgegevens en het gebruik van ICT. Tevens is deze regeling onlosmakelijk verbonden met de geldende gedragscode binnen de Scholengroep Katholiek Onderwijs Flevoland en Veluwe (SKO).

Binnen de regeling zijn er zaken waarmee wij rekenen zullen moeten houden.

Wettelijke bepalingen overheid

De overheid heeft al gezorgd voor een eerste afbakening. Denk hierbij aan wetgeving met betrekking tot privacy, auteursrecht, beeldschermgebruik en verspreiding van virussen.

Voor het gebruik van elektronische informatie- en communicatiemiddelen (EIC) door personeel van de SKO is de regeling vastgesteld door het College van Bestuur van de SKO.

Deze regeling geeft de wijze aan waarop binnen de instelling/school door de schoolleiding wordt omgegaan met elektronische informatie- en communicatiemiddelen. Vanuit de SKO is het van belang dat deze wettelijke bepalingen en deze regeling worden nageleefd. Immers; scholen hebben een voorbeeldfunctie.

¹ Onderstaande wetgeving heeft gevolgen voor het dagelijks gebruik van computers en Internet binnen de SKO

1. De Wet Computercriminaliteit
2. De Wet Beeldschermgebruik
3. De Wet Bescherming Persoons(registratie)gegevens
4. Artikel 350 Wetboek van Strafrecht ziet toe op het wissen, veranderen, dan wel het onbruikbaar of ontoegankelijk maken van gegevens.
5. In Artikel 350b lid 2 van het Wetboek van Strafrecht wordt het verspreiden van virussen door onvoorzichtigheid, onachtzaamheid of nalatigheid strafbaar gesteld.
6. In Europees verband is in het verdrag "Crime in Cyberspace" van de Raad van Europa een strafbaarstelling met betrekking tot het verspreiden van virussen opgenomen.
7. De Wet auteursrecht.
8. De Wet portretrecht.

Artikel 1 Doel en werkingssfeer van deze regeling

- 1.1 Deze regeling geeft de wijze aan waarop binnen de SKO wordt omgegaan met elektronische informatie- en communicatiemiddelen (EIC). Deze regeling omvat gedragsregels ten aanzien van verantwoord gebruik en geeft regels over de wijze waarop controle plaats vindt.
- 1.2 Onverantwoord gebruik is gebruik tegenstrijdig aan de doelstelling en identiteit van de school, zowel in persoonlijk gebruik als in relatie tot anderen binnen of buiten de school. Hierbij wordt in het bijzonder gedacht aan illegale toepassingen van bestanden, godslasterlijke, beledigende, aanstootgevende, gewelddadige, racistische, discriminerende, intimiderende, pornografische toepassingen, zinloos tijdverdrijf en /of toepassingen die strijdig zijn met de wet of als onethisch (niet fatsoenlijk, onzedelijk gedrag) te karakteriseren zijn.
- 1.3 De controle op persoonsgegevens bij gebruik van elektronische informatie- en communicatiemiddelen vindt plaats met als doel:
 - a. systeem- en netwerkbeveiliging en
 - b. tegengaan onverantwoord gebruik.
- 1.4 Deze regeling geldt voor een ieder die ten behoeve van de school werkzaamheden verricht.

Artikel 2 Algemene uitgangspunten

- 2.1 De controle op gebruik van elektronische informatie- en communicatiemiddelen zal overeenkomstig deze regeling uitgevoerd worden.
- 2.2 Gestreefd wordt naar een goede balans tussen controle op verantwoord gebruik en bescherming van de privacy van personeelsleden op de werkplek.
- 2.3 Persoonsgegevens over gebruik van elektronische informatie- en communicatiemiddelen worden niet langer bewaard dan noodzakelijk, met een maximum bewaartermijn van 6 maanden.
- 2.4 Het bestuur & de schoolleiding treffen voorzieningen over de positie en integriteit van de ICT-beheerorganisatie. Dit wordt geconcretiseerd door de beheerorganisatie alleen technisch verantwoordelijk te laten zijn. Dit laat onverlet het bepaalde in artikel 5.5.

Artikel 3 Gebruik van elektronische informatie- en communicatiemiddelen

- 3.1 Het gebruik van elektronische informatie- en communicatiemiddelen is primair verbonden met taken/bezigheden die voortvloeien uit de functie van het personeelslid. E-mail-communicatie heeft slechts plaats via het persoonlijke werkaccount van de medewerker in Office 365. Gedragsregels die gelden voor het ondertekenen van schriftelijke correspondentie, het vertegenwoordigen van de school, het verzenden van post, zijn ook van toepassing op gebruik van elektronische informatie- en communicatiemiddelen.
- 3.2 Personeelsleden mogen elektronische informatie- en communicatiemiddelen beperkt, incidenteel en kortstondig gebruiken voor persoonlijke doeleinden mits dit niet storend is voor de dagelijkse werkzaamheden of het systeem en mits hierbij wordt voldaan aan de verdere regels van deze regeling.
- 3.3 Het is niet toegestaan om elektronische informatie- en communicatiemiddelen zodanig te gebruiken dat het systeem- en/of de beveiliging opzettelijk worden aangetast, of de inhoudelijke communicatie tegenstrijdig is aan de doelstelling en identiteit zoals omschreven in artikel 1.2.
- 3.4 Het is niet toegestaan om elektronische informatie- en communicatiemiddelen voor onacceptabele doeleinden te gebruiken. Hierbij moet onder andere worden gedacht aan het spelen of downloaden van spelletjes, winkelen, gokken of deelnemen aan kansspelen en het bezoeken van chatboxen.

3.5 Het is in het bijzonder niet toegestaan om:

- bewust sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten;
- bewust pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal te bekijken of te downloaden of te verspreiden;
- bewust informatie waartoe men via elektronische informatie- en communicatiemiddelen toegang heeft verkregen zonder toestemming te veranderen of te vernietigen;
- actief aan te geven aan webwinkels dat belangstelling bestaat voor het ontvangen van productinformatie voor eventuele latere bestellingen in de privésfeer;
- bestanden te downloaden die geen verband houden met studie en/of werk;
- software en applicaties te downloaden zonder voorafgaande toestemming van de beheerder;
- niet-educatieve spelletjes te spelen buiten de pauzes;
- anoniem of onder een fictieve naam via elektronische informatie- en communicatiemiddelen te communiceren;
- op dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende manier via elektronische informatie- en communicatiemiddelen te communiceren;
- buiten de pauzes inkomende privé-berichten te genereren;
- een telefoon van de school te gebruiken in of naar het buitenland zonder uitdrukkelijke toestemming van het bevoegd gezag;
- iemand lastig te vallen.

3.6 Het is niet toegestaan om zonder toestemming foto's, video's of ander materiaal van op school werkzame personen of leerlingen of andere bij de school betrokkenen via elektronische informatie- en communicatiemiddelen bekend te maken. Voor het bekend maken van foto's, video's, filmpjes e.d. waarop personen zijn afgebeeld is voorafgaande toestemming van betrokkene of diens wettelijke vertegenwoordiger vereist.

3.7 Het is ook anderszins niet toegestaan om door middel van elektronische informatie- en communicatiemiddelen in strijd met de wet of onethisch te handelen.

3.8 User-identificatie (gebruikersnaam) en authenticatie (bijvoorbeeld wachtwoord) zijn persoonsgebonden en mogen niet aan anderen worden doorgegeven.

3.9 Onbedoelde inbreuken op beveiliging, van binnenuit of van buiten de school dienen onmiddellijk aan de systeembeheerder gemeld te worden.

Artikel 4 Meldingsplicht

Een vermoeden van misbruik van elektronische informatie- en communicatiemiddelen moet direct worden gemeld bij schoolleiding of voorzitter van het bevoegd gezag.

Artikel 5 Controle

5.1 Controle op gebruik van elektronische informatie- en communicatiemiddelen vindt slechts plaats in het kader van in artikel 1.2 en 1.3 genoemde doelen.

5.2 De (bovenschoolse) schoolleiding informeert de personeelsleden voorafgaand aan de invoering van de regeling over controle op elektronische informatie- en communicatiemiddelen, omtrent de doeleinden, de aard van de gegevens, de omstandigheden waaronder zij verkregen zijn en de inhoud van deze regeling.

5.3 Niet toegestaan gebruik van elektronische informatie- en communicatiemiddelen wordt zo veel mogelijk technisch onmogelijk gemaakt.

- 5.4 Controle vindt, door de schoolleiding in overleg met het CvB, bij een vermoeden van misbruik plaats.
- 5.5 Als een lid van de (bovenschoolse) schoolleiding of de ICT-beheerorganisatie merkt, of er op geattendeerd wordt, dat het EIC-gedrag van een personeelslid niet binnen deze kaders verloopt, wordt de collega hier op gewezen en wordt een controle van zijn EIC-acties door bevoegde personen als mogelijkheid genoemd.
- 5.6 Elektronische informatie- en communicatieberichten van de (bovenschoolse) schoolleiding, bestuursleden, vertrouwenspersonen en andere personeelsleden met een vertrouwensfunctie, zijn in beginsel uitgesloten van controle. Dit geldt niet voor de controle bij een ernstig vermoeden van misbruik.
- 5.7 Als er een onderbouwd vermoeden bestaat van het oneigenlijk gebruik van EIC vindt gepersonaliseerde controle plaats. De rapportage wordt verstrekt aan de (bovenschoolse) schoolleiding en aan de ICT-beheerorganisatie. De schoolleiding meldt dit aan het bestuur.
- 5.8 Het bestuur geeft indien nodig aan de ICT-beheerorganisatie de opdracht om de elektronische informatie- en communicatiemiddelenacties van de betrokkene(n) na te gaan.
- 5.9 De ICT-beheerorganisatie brengt hiervan schriftelijk verslag uit aan het bestuur.
- 5.10 Personeelsleden, ten aanzien van wie geconstateerd is dat zij zich niet aan deze regeling houden, worden zo spoedig mogelijk door de leidinggevende op hun gedrag aangesproken.
- 5.11 Bij handelen in strijd met deze regeling beslist het bestuur over de al dan niet te nemen (disciplinaire) maatregelen. Tot deze maatregelen kan ontslag uit het dienstverband behoren.

Artikel 6 Inwerkingtreding en citeertitel

Deze regeling kan aangehaald worden als EIC-regeling voor personeel en treedt in werking op **1 oktober 2016**.

De EIC-regeling is vastgesteld door het bevoegd gezag van de SKO en vervangt eventuele vorige versies.

Toelichting op de EIC- modelregeling

De EIC-modelregeling betreft het gebruik van (mobiele) telefoon, internet, e-mail en andere huidige en toekomstige elektronische informatie- en communicatiemiddelen zoals deze ter beschikking worden gesteld of worden gefinancierd door de SKO (als werkgever). In de tekst wordt hiernaar in algemene zin verwezen als "*elektronische informatie- en communicatiemiddelen*".

Een aantal organisaties voor bestuur en management in het PO en VO, te weten Verus, VKO, VBS en VGS, heeft gezamenlijk de voorliggende modelregeling opgesteld.

Een belangrijk punt is de totstandkoming van een goede balans tussen verantwoord gebruik van deze elektronische informatie- en communicatiemiddelen en bescherming van de privacy van iedereen die op school werkzaamheden verricht en achter de pc zit (dus ook vrijwilligers, stagiaires, enz.).

De tekst van de modelregeling sluit op dat punt aan bij de Wet Bescherming Persoonsgegevens. Belangrijk is dat de Wbp alleen geldt als er sprake is van persoonsgegevens. Gegevens met betrekking tot bijvoorbeeld e-mail- en internetgebruik van personeel zijn in het algemeen te kwalificeren als persoonsgegevens. Een IP-adres is in principe te herleiden tot een bepaalde gebruiker. Een specifieke brochure over internetgebruik op de werkplek is bij het College Bescherming Persoonsgegevens op te vragen.

Het model is niet van toepassing op het gebruik van elektronische informatie- en communicatiemiddelen door leerlingen.

Op grond van art. 7:660 BW is de werkgever gerechtigd tot het geven van voorschriften voor het verrichten van de arbeid en het nemen van maatregelen ter bevordering van de goede orde in de onderneming (in dit geval de school).

Gebaseerd op dit artikel kan de school (werkgever) overgaan tot het reguleren en controleren van e-mail en internet. Veel scholen kiezen ervoor een reglement op te stellen waarin afspraken zwart op wit worden gezet over met name internet en e-mailgebruik. De school (werkgever) en het personeel hebben dan schriftelijke afspraken waarin duidelijk staat wat wel en wat niet kan. Op deze manier kan de school (werkgever) een inschatting maken tot hoever hij gaan kan met het maken van inbreuken op de privacy van op school werkzame personen. Laatstgenoemden hebben dan een houvast hoe vaak en op welke manier ze internet en e-mail gebruiken kunnen.

Uit rechterlijke uitspraken is op te maken dat er veel waarde gehecht wordt aan het hebben van een reglement of protocol. Hierdoor weet het personeel immers waar het aan toe is. Belangrijk is ook dat dit duidelijk kenbaar gemaakt wordt aan het personeel; bijvoorbeeld bij het inloggen.

Zorg dus dat iedereen die op school werkzaam is de regeling kent, bijvoorbeeld door de regeling aan alle personeelsleden op papier en/of via e-mail te sturen, door publicatie in een personeelsnieuwsbericht, via een meldtekst op het scherm, bij het uitreiken van een e-mailadres of een nieuwe mobiele telefoon e.d. Opnemen in het personeelsreglement of het equivalent daarvan is uiteraard ook aanbevelenswaardig.

Artikelsgewijze toelichting

Artikel 1 Doel van deze regeling

Deze regeling is van toepassing op personen in dienst van of werkzaam voor de school: zij die ten behoeve van de school werkzaamheden verrichten. Hieronder vallen niet alleen de personen die een akte van benoeming/aanstelling hebben, maar ook uitzendkrachten, stagiaires, vrijwilligers, personen die bij de school zijn gedetacheerd, etc. In de tekst wordt geregeld het woord personeelslid gebruikt maar hier worden dus alle personen bedoeld die in dienst van of werkzaamheden ten behoeve van de school verrichten.

Artikel 2 Algemene uitgangspunten

De maximale bewaartermijn van 6 maanden geldt specifiek in het kader van deze regeling; relevante informatie die opgenomen dient te worden in een (personeels)dossier, valt onder de werking van de Wbp en kan uit dien hoofde langer worden bewaard. Als er bijvoorbeeld naar aanleiding van een controle reden is om met een personeelslid in gesprek te treden, een waarschuwing te geven, etc. zal dit uiteraard in het personeelsdossier worden vastgelegd (zie ook artikel 5).

In deze modelregeling is gekozen voor het algemene begrip ICT-beheerorganisatie. Desgewenst kunt u in de regeling van uw school hiervan afwijken door meer aan te sluiten bij de functies die op uw school zijn vastgesteld. In het basisonderwijs wordt veelal de omschrijving ICT-coördinator of I-coach gehanteerd.

In deze regeling is ervoor gekozen de ICT-coördinator/I-coach enkel een technische, signalerende verantwoordelijkheid toe te delen. Daarmee kan voorkomen worden dat de ICT-beheerorganisatie in een loyaliteitsconflict komt met één van zijn collega's. Bij een vermoeden van misbruik van de EIC-middelen van de school wordt het desbetreffende personeelslid door of namens de schoolleiding hierop gewezen (zie ook artikel 5.5. van de modelregeling). Het verdient aanbeveling deze taak niet te mandateren aan de ICT-beheerorganisatie.

Omdat de ICT-beheerorganisatie toegang heeft tot bijna alle gegevens binnen ons netwerk en de portaalomgeving (Office 365) moet de functie met de nodige waarborgen omgeven zijn. Zo heeft hij, net als overigens al het personeel maar op grond van de aard van zijn werkzaamheden in het bijzonder, een geheimhoudingsplicht. Ook is hij niet bevoegd tot het lezen van e-mail of het real-time meekijken zonder dat daartoe een aanleiding is. De ICT-beheerorganisatie moet tegenover de (boven)school(se) leiding of het bestuur een zekere onafhankelijkheid hebben. Hij mag niet door de (boven)school(se) leiding of het bestuur gedwongen worden af te wijken van procedures die de zorgvuldigheid van het proces bewaken.

Artikel 3 Gebruik van elektronische informatie- en communicatiemiddelen

Een totaal verbod op het privégebruik van elektronische informatie- en communicatiemiddelen zoals het versturen en ontvangen van persoonlijke e-mailberichten is niet reëel. De school kan wel beperkende voorwaarden stellen aan het privégebruik.

In de modelregeling kunnen gedragsregels worden opgenomen over wat er in de school onder bijvoorbeeld verantwoord e-mailgebruik wordt verstaan:

- een correcte vermelding van afzender;
- het meesturen van een disclaimer;
- duidelijke onderwerp aanduiding;
- terughoudend omgaan met vertrouwelijke gegevens en gevoelige informatie.

Voorbeelden van niet toegestaan gebruik zijn:

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

Als de inhoud van een e-mail in ernstige mate ontoelaatbaar is (opruiend, hatelijk, onsmakelijk etc.), of de wet overtreedt (bijvoorbeeld door valse beschuldigingen te doen), neem dan contact op met de politie. Print de e-mail uit en bewaar een (digitale) kopie als potentieel bewijsmateriaal. Let op: het adres waar een e-mail vandaan komt is te vervalsen, dus de werkelijke afzender kan zijn/haar identiteit onder iemand anders' naam verborgen houden.

Telewerken is niet apart vermeld in deze modelregeling. De controle door de werkgever van het computergebruik van het personeel vormt in situaties waarin het personeelslid vanuit zijn eigen huis inlogt op het computersysteem (Office 365 en de portalen) van de school (telewerken) een extra probleem. Voor zover het personeelslid uitsluitend ten behoeve van het werk inlogt, zullen de regels in deze regeling van overeenkomstige toepassing zijn. De computer van het personeelslid thuis maakt dan immers logisch gezien deel uit van het computernetwerk en het personeelslid bevindt zich in een situatie waarin ook de gezagsbevoegdheid van de werkgever geldt.

Dit is anders als het personeelslid de schoolaccount kan en mag gebruiken om privé e-mail te versturen of in zijn eigen tijd over het internet te surfen. Voor logging van hetgeen hij privé doet, is veelal geen grond. Dit geldt zeker indien ook zijn gezinsleden van de faciliteiten gebruik mogen maken. Met hen heeft de school (werkgever) immers geen arbeidsrelatie waarin hij zijn gezag kan uitoefenen. Zijn positie is in deze situatie vergelijkbaar met een provider.

Adviseer personeel om niet te antwoorden op junkmail, omdat de kans groot is dat men er nog meer van ontvangt als men het wel doet. Wees voorzichtig met het bekend maken van het e-mailadres op websites, bijvoorbeeld bij het invullen van een formulier. Ook bij het invullen van het huisadres in publieke gebieden, zoals bijvoorbeeld een 'gastenboek', is voorzichtigheid geboden. Pas op met e-mailberichten waar grote bestanden als attachment zijn bijgevoegd, met name als ze afkomstig zijn van mensen die men niet kent of met onderwerptitels die niets zeggen. Verwijder iedere verdacht bericht en leeg de e-mail prullenbak.

Nog één tip:

Besteed als school aandacht aan beveiliging van uw netwerk. Abonneer u als school op waarschuwingdiensten. De Nederlandse overheid heeft www.veiliginternetten.nl, waar men zich kan aanmelden voor gratis e-mail-berichten wanneer er lekken zijn ontdekt, nieuwe virussen, e.d..

Artikel 5 Controle

Het gebruik van elektronische informatie- en communicatiemiddelen leidt per verschijningsvorm tot andere risico's voor de school en het personeelslid. Voor de school kan het gaan om de beveiliging van het netwerk, het tegengaan van 'verboden gebruik' of het beschermen van andere belangen zoals de goede naam van de organisatie. Voor het personeelslid staat vaak het privacybelang door de controle onder druk, maar ook de vrijheid van meningsuiting of de informatievrijheid kan in het geding zijn. Als werkgever zal men zich hier bewust van dienen te zijn als men overgaat tot controle van bijvoorbeeld e-mail- en internetgebruik van personeel.

Als grondslag van de controle kan doorgaans worden aangewezen het gerechtvaardigd belang van de school (werkgever). Hierbij geldt wel dat hij een aantoonbare belangenafweging moet maken tussen zijn belangen en de (privacy) belangen van het personeel. De aard, omvang en de vorm van de controlemaatregelen dienen derhalve in een redelijke verhouding te staan tot het doel van de controle.

De controlemaatregelen dienen beperkt te zijn en dienen gegevens niet onnodig vast te leggen. Indien het doel de vastlegging van gegevens op persoonsniveau niet vereist, moet worden volstaan met geaggregeerde of geanonimiseerde gegevens.

Een ander punt is waarvoor de gegevens die door middel van de controle zijn verzameld, mogen worden gebruikt. Deze doelen mogen niet onverenigbaar zijn met het doel waarvoor de gegevens zijn verkregen. Dit ligt anders bij incidenteel gebruik van de gegevens wegens verdenking van overtreding van de regels. In dat geval zal een school als werkgever er toe over mogen gaan om de gegevens voor zijn onderzoek te gebruiken als dat noodzakelijk is voor voorkoming, opsporing of vervolging van strafbare feiten binnen de organisatie. Daarbij dient hij wel zorgvuldig te werk te gaan en de controlemiddelen naar evenredigheid in te zetten.

De werkgever is verplicht om het personeel inlichtingen te verschaffen over het doel van de controlemiddelen, de manier waarop de gegevens worden verkregen en het gebruik dat ervan wordt gemaakt. Transparantie is een belangrijk beginsel voor privacybescherming. De informatieplicht is - afhankelijk van de situatie- gebaseerd op de artikelen 33 en 34 WBP. De verplichting vloeit ook voort uit de Arbowetgeving. Het enkele overleg met de (G)MR is in dit kader onvoldoende. Het personeel moet individueel worden voorgelicht. In geval van e-mail- en internetcontrole is het moment van inloggen hiervoor het aangewezen tijdstip.

Het personeelslid heeft het recht op inzage in de gegevens. Hij kan verder de werkgever verzoeken de gegevens aan te vullen, te verbeteren, te verwijderen of af te schermen indien deze feitelijk onjuist zijn, voor het doel onvolledig of niet ter zake dienend zijn dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt. Tenslotte kan het personeelslid tegen de verwerking van zijn persoonsgegevens verzet aantekenen in verband met zijn bijzondere persoonlijke omstandigheden.

Via het managementstatuut kan dit gemandateerd worden aan de (bovenschoolse) schoolleiding.

Als er een vermoeden is op grond waarvan een gepersonaliseerde controle plaatsvindt, wordt het bovenschoolse niveau of het bestuur ingeschakeld (zie artikel 5.9).

Zie ook de toelichting bij artikel 2 lid 3.

Als een school niet beschikt over gedragsregels ten aanzien van het gebruik van elektronische- informatie- en communicatiemiddelen, mag desalniettemin van het personeel worden verwacht dat zij weten wat acceptabel is of niet en daar naar handelen. De afwezigheid van een dergelijk beleid is nog geen rechtvaardiging voor een ontoelaatbare handelwijze van betrokken personeelsleden. Toch zal het voor een school als werkgever verstandig zijn om een duidelijk beleid te hebben. De aanwezigheid van een expliciete regeling zal waarschijnlijk als relevante factor meewegen in een eventuele ontslagprocedure.