



EIC-protocol

(Protocol elektronische informatie- en communicatiemiddelen)

Onderwerp / voorstel:	Protocol elektronische informatie- en communicatiemiddelen	Status:	definitief
Periode:	September 2011 – juli 2014	Versienr:	1.0
Code:		# Pagina's:	9
Eigenaar:	Sonja van Katwijk		
Akkoord:	MT	Datum:	25-8-2011
	MR	Datum:	20-9-2011
	Bestuur	Datum:	1-9-2011
Bijlagen:	geen		



Inhoudsopgave

Inhoudsopgave	2
1 Inleiding.....	3
2 Artikelen	3
Artikel 1 – Doel en werkingssfeer van dit protocol.....	3
Artikel 2 – Algemene uitgangspunten	4
Artikel 3 – Gebruik van elektronische informatie- en communicatiemiddelen	4
Artikel 4 – Meldingsplicht	5
Artikel 5 – Controle	5
3 Aanvulling betreffende afspraken over elektronische communicatie en profilering op internet	6
4 Overgangsregeling.....	6
5 Toelichting op het EIC- protocol	7
Artikelgewijze toelichting.....	7
Artikel 1 – Doel van deze regeling	7
Artikel 2 – Algemene uitgangspunten	7
Artikel 3 – Gebruik van elektronische informatie- en communicatiemiddelen	8
Artikel 5 – Controle	9

1 Inleiding

Door het steeds intensievere gebruik van elektronische informatie- en communicatiemiddelen is er meer en meer noodzaak gekomen om ouders en teamleden van de Kosmos richtlijnen te geven omtrent het gebruik van deze middelen. Dit protocol biedt duidelijkheid en zekerheid voor iedereen.

Ex ante: dit protocol is niet bedoeld om het gebruik van moderne middelen te beperken, maar om richtlijnen mee te geven bij het gebruik van of het exploreren van moderne middelen.

Dit protocol is ons aangereikt door stichting Meerkring en daar waar nodig aangepast aan de Kosmos.

2 Artikelen

Artikel 1 – Doel en werkingssfeer van dit protocol

- 1.1 Deze regeling geeft de wijze aan waarop binnen de Kosmos (zowel de schoolvereniging als de school) wordt omgegaan met elektronische informatie- en communicatiemiddelen (EIC). Deze regeling omvat gedragsregels voor teamleden en ouders 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 vereniging en de school, zowel in persoonlijk gebruik als in relatie tot anderen binnen of buiten de vereniging en 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 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
 - b. tegengaan onverantwoord gebruik.
- 1.4 Deze regeling geldt voor een ieder die ten behoeve van de vereniging of school werkzaamheden verricht.

Artikel 2 – Algemene uitgangspunten

De controle op gebruik van elektronische informatie- en communicatiemiddelen zal overeenkomstig deze regeling worden uitgevoerd.

Daar waar staat 'personeelslid' wordt bedoeld:

1. personeelsleden van de Kosmos
2. stagiaires die op de Kosmos werkzaam zijn
3. externen, die ingehuurd zijn door en werkzaam zijn op de Kosmos
4. ouders van de Kosmos, voor zover hun taken/bezigheden verband houden met werkzaamheden voor de school of schoolvereniging
5. vrijwilligers

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 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 voor schoolgebruik, 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 voor privé-doeleinden, gokken of deelnemen aan kansspelen, het voeren van een werkgerelateerd dagboek 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;
 - zich tot niet openbare bronnen op het internet toegang te verschaffen;
 - 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 privé-sfeer;
 - 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;
 - 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;
 - zich negatief uit te laten over derden, ook zijnde leerlingen, ouders, Kosmosmedewerkers;
 - inkomende privé-berichten te genereren door het deelnemen aan niet-zakelijke nieuwsgroepen, abonnementen op e-zines, elektronisch winkelen, down- en uploaden van bestanden, nieuwsbrieven en dergelijke;
 - kettingmailberichten te verzenden of door te sturen;
 - iemand lastig te vallen.

- 3.6 Het is niet toegestaan om 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 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 directie gemeld te worden.

Artikel 4 – Meldingsplicht

Een vermoeden van misbruik van elektronische informatie- en communicatiemiddelen moet direct worden gemeld bij de directie van school of stichting.

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 directie informeert de personeelsleden voorafgaand aan de invoering van dit protocol 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 in beginsel plaats bij vermoeden van misbruik door de ict-coördinator en een directielid samen.
- 5.5 Als een lid van de directie of de ict-coördinator merkt of er op wordt geattendeerd dat het EIC-gedrag van een personeelslid niet binnen deze kaders verloopt, wordt de collega door de directie hier op gewezen en wordt een controle van zijn EIC-acties door bevoegde personen als mogelijkheid genoemd.
- 5.6 Indien een personeelslid of een groep personeelsleden ervan wordt verdacht de regels te overtreden, meldt de directie dit aan het bestuur.
- 5.7 Het bestuur geeft indien nodig aan de directeur de opdracht om de elektronische informatie- en communicatiemiddelenacties van de betrokkene na te gaan.
- 5.8 De directie brengt hiervan schriftelijk verslag uit aan het bestuur.
- 5.9 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.
- 5.10 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.

3 Aanvulling betreffende afspraken over elektronische communicatie en profilering op internet

Binnen de Kosmos gelden gedragsregels ten aanzien van het gebruik van elektronische informatie- en communicatiemiddelen op school (zoals computers en email). Praktijk leert echter dat ook het gebruik van internet en e-mail in het algemeen tot onverwachte en ongewenste situaties kan leiden voor individuele werknemers, ook wanneer hierbij niet gebruik wordt gemaakt van de middelen die door de werkgever beschikbaar zijn gesteld. Ter bescherming van de individuele integriteit van het personeel en De Kosmos als organisatie, gelden er voor het personeel van de Kosmos twee aanvullende gedragsregels voor elektronisch berichtenverkeer en profilering op internet:

- 1) De wijze waarop een personeelslid zich profileert op internet is verenigbaar met de gedragsregels binnen de school en de vereniging en/of mag voorts de goede vervulling van de functie door het personeelslid of het goed functioneren van de school of de vereniging niet belemmeren of schaden.
- 2) Een personeelslid beperkt zich in het elektronisch berichtenverkeer met leerlingen tot functionele berichten. Bij elektronische communicatie met leerlingen wordt uitsluitend gebruik gemaakt van de email adressen van de school resp. de mogelijkheden binnen de elektronische leeromgeving van school (ELO)..

Toelichting op de aanvullende gedragsregels:

De wijze waarop een personeelslid zich profileert op internet is verenigbaar met de gedragsregels binnen de school en de vereniging.

Ongewenste profilering op internet kan leiden tot onrust, imagoschade of kwetsbaarheid van het betreffende personeelslid, school en/of vereniging. Onder profilering wordt bijvoorbeeld verstaan: informatie op een eigen website (weblog), deelname aan een gebruikersnetwerk (zoals Hyves) en reacties op een forum/prikbord. Het gaat hierbij om informatie waarbij achterhaald kan worden dat het betrekking heeft op (of geschreven is door) een personeelslid.

Een personeelslid beperkt zich in het elektronisch berichtenverkeer met leerlingen tot functionele berichten. Bij elektronische communicatie met leerlingen wordt uitsluitend gebruik gemaakt van de e-mailadressen van de school.

Voor het versturen van elektronische berichten naar leerlingen wordt uitsluitend gebruik gemaakt van het e-mailadres van de school (of stichting) of de ELO-faciliteiten. Dit betekent dat het gebruik van andere media voor het versturen en ontvangen van elektronische berichten (zoals een privé e-mailadres, SMS, chat-programma's) niet toegestaan is.

Het elektronische berichtenverkeer tussen personeel en leerlingen dient beperkt te blijven tot berichten die in essentie betrekking hebben op onderwijs en onderwijsgerelateerde zaken. Het is niet de bedoeling dat elektronisch berichtenverkeer wordt gebruikt voor gesprekken tussen personeel en leerlingen over andere zaken (zoals hobby's, emoties, privé-aangelegenheden en algemene belangstelling).

In bijzondere gevallen (zoals in het geval van langdurige afwezigheid van een leerling of van een personeelslid) kan er worden besloten om af te wijken van deze algemene gedragsregels. Een dergelijke beslissing wordt altijd genomen door de directie en met goedkeuring van ouders.

4 Overgangsregeling

Tot 3 maanden na het in werking treden van dit document krijgen alle zittende personeelsleden de gelegenheid hun school e-mailadres te schonen en privacygevoelige informatie te verwijderen c.q. over te zetten op een privé e-mailadres.

5 Toelichting op het EIC- protocol

Het EIC-protocol 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 Kosmos (als werkgever). In de tekst wordt hiernaar in algemene zin verwezen als "*elektronische informatie- en communicatiemiddelen*".

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 dit protocol 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.

Dit protocol 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 het protocol kent, bijvoorbeeld door de regeling aan alle personeelsleden op papier en/of via e-mail te sturen, door publicatie in een personeelsnieuwsbrief, via een meldtekst op het scherm en/of bij het uitreiken van een e-mailadres.

Artikelgewijze 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

Lid 3

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).

Lid 4

In deze regeling is ervoor gekozen de ict-coördinator enkel een technische, signalerende verantwoordelijkheid toe te delen. Daarmee kan voorkomen worden dat een ict-coördinator 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 directie hierop gewezen (zie ook artikel 5.5.). Het verdient aanbeveling deze taak niet te mandateren aan de ict-coördinator.

Omdat een ict-coördinator toegang heeft tot bijna alle gegevens binnen het computernetwerk 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-coördinator moet tegenover de (algemene) directie of het managementteam een zekere onafhankelijkheid hebben. Hij mag niet door de (algemene) directie of het managementteam gedwongen worden af te wijken van procedures die de zorgvuldigheid van het proces bewaken. Bij steekproefsgewijze controle van het gebruik van elektronische informatie- en communicatiemiddelen wordt de ict-coördinator bijgestaan door een directielid.

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 regeling 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 onderwerpaanduiding;
- 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 (opruierend, 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.

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 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. De Kosmos adviseert haar werknemers dan ook geen gebruik te maken van het school e-mail adres voor privé zaken.

De Kosmos adviseert haar werknemers 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 bijlage 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.

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 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. 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.

Lid 9, lid 11 en lid 13

Via het managementstatuut kan dit gemandateerd worden aan de directie van de school.

Lid 9

Als er een vermoeden is op grond waarvan een gepersonaliseerde controle plaatsvindt, wordt het managementteam ingeschakeld (zie artikel 5.9). Zie ook de toelichting bij artikel 2 lid 3.