Elektronische informatie- en communicatiemiddelen (EIC)-regeling

Stichting Confessioneel Onderwijs Leiden

Vastgesteld door het College van Bestuur: 19 november 2013

Instemming GMR Primair Onderwijs: 25 november 2013

Instemming GMR Voortgezet Onderwijs: 17 december 2013

Inwerkingtreding: 1 januari 2014

Inhoud

Inleiding 3

Paragraaf 1. Begripsbepalingen 4

Paragraaf 2. Doel en werkingssfeer 5

Artikel 1. Doel en werkingssfeer van deze regeling 5

Artikel 2. Algemene uitgangspunten 5

Paragraaf 3. Gebruik 5

Artikel 3. Gebruik van elektronische informatie- en communicatiemiddelen 5

Paragraaf 4. Melding en controle 7

Artikel 4. Meldingsplicht 7

Artikel 5. Controle 7

Artikel 6. Inwerkingtreding en citeertitel 7

Paragraaf 5. Toelichting op de EIC- modelregeling 8

Paragraaf 6. Artikelsgewijze toelichting 10

Artikel 1. Doel van deze regeling 10

Artikel 2. Algemene uitgangspunten 10

Artikel 3. Gebruik van elektronische informatie- en communicatiemiddelen 10

Artikel 5. Controle 11

Referenties 13

Verklarende woordenlijst 14

Inleiding

Het gebruik van elektronische informatie- en communicatiemiddelen heeft een enorme vlucht genomen. Het gebruik van die middelen biedt ons meer mogelijkheden voor een betere communicatie.
Binnen de scholen gebruiken we de communicatiemiddelen voor:

- het leerproces van leerlingen en medewerkers;
- het voeren van verschillende administraties;
- het communicatieverkeer dat op het werk en het leren gericht is;
- de communicatie die nodig is voor een goede bedrijfsvoering.

Ondertussen is gebleken dat het ook mogelijk is die middelen te misbruiken of onbewust op een manier te gebruiken die de goede werking van de middelen verstoort. In het verleden is gebleken dat de middelen soms zo ingezet worden dat er schade wordt berokkend aan medegebruikers of aan de Stichting en/of haar scholen. Ook komt het voor dat vaak onbewust de werking van het systeem enorm vertraagd wordt doordat grote bestanden gedownload worden of naar beeld of audiostreams gekeken of geluisterd wordt.

Om misbruik van de eigen en/of stichtingscommunicatiemiddelen aan te kunnen pakken is dit reglement opgesteld.
Hieronder staat de regeling waarvan alle medewerkers geacht worden de inhoud te kennen en binnen de kaders ervan te blijven handelen. Dit reglement is alleen van toepassing op personeel.

Paragraaf 1. Begripsbepalingen

a.) Stichting: Stichting Confessioneel Onderwijs Leiden;

b.) Personeel: bij of voor het bevoegd gezag werkende personen;

c.) EIC: elektronische informatie- en communicatiemiddelen;

d.) Systeembeheerder: ICT-coördinator/ ICT-er;

e.) CBP: College Bescherming Persoonsgegevens;

f.) Wbp: Wet bescherming persoonsgegevens, wet van 6 juli 2000 (Staatsblad 2000, 302;

Paragraaf 2. Doel en werkingssfeer

Artikel 1. Doel en werkingssfeer van deze regeling

1.1 Deze regeling geeft de wijze aan waarop in de **Stichting Confessioneel Onderwijs leiden** 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 plaatsvindt.

1.2 Onverantwoord gebruik is gebruik tegenstrijdig aan de doelstelling en identiteit van de Stichting, zowel in persoonlijk gebruik als in relatie tot anderen binnen of buiten de Stichting. Hierbij wordt in het bijzonder gedacht aan illegale toepassingen van bestanden, godslasterlijke, beledigende, aanstootgevende, gewelddadige, racistische, discriminerende, intimiderende, pornografische toepassingen 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. de systeem- en netwerkbeveiliging;

b. het tegengaan van onverantwoord gebruik.

1.4 Deze regeling geldt voor een ieder die ten behoeve van de Stichting 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 De directie treft voorzieningen voor de positie en integriteit van de systeembeheerder en andere personen die beheer voeren over en toegang hebben tot informatiesystemen. Dit wordt geconcretiseerd door deze personen alleen technisch verantwoordelijk te laten zijn en dit laat onverlet het bepaalde in artikel 5.5.

Paragraaf 3. Gebruik

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 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 dit reglement.

3.3 Het is niet toegestaan om elektronische informatie- en communicatiemiddelen zodanig te gebruiken dat het systeem- en/of de beveiliging opzettelijk wordt 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, het voeren van een werk gerelateerd dagboek (bloggen) en het bezoeken van chatboxen. Ook het online luisteren naar radio en het bekijken van televisie en andere video-online toepassing valt onder deze noemer.
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 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;
- anoniem of onder een fictieve naam via elektronische informatie- en communicatiemiddelen te communiceren;
- op een dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende manier via elektronische informatie- en communicatiemiddelen te communiceren;
- 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 tenzij deze vakgerelateerd zijn.
- kettingmailberichten te verzenden of door te sturen;
- een mobiele telefoon van de school te gebruiken in het buitenland zonder uitdrukkelijke toestemming van het bevoegd gezag;
- iemand lastig te vallen;
- met behulp van bewakingscamera's verkregen beeldmateriaal te gebruiken voor andere doeleinden dan het voorkomen of opsporen van schade aan personen of goederen.

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, video's of ander materiaal waarop medewerkers zijn afgebeeld is voorafgaande toestemming van betrokkene vereist. Op foto's, video's of ander materiaal waarop leerlingen zijn afgebeeld komen alleen die leerlingen voor waarvan de ouders of wettelijke vertegenwoordigers schrijftelijke toestemming gegeven. Deze toestemming is niet vereist voor beeldmateriaal van bewakingscamera's dat gebruikt wordt voor het doen van aangifte van een strafbaar feit.
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-identifcatie (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.

Paragraaf 4. Melding en controle

Artikel 4. Meldingsplicht
Een vermoeden van misbruik van elektronische informatie- en communicatiemiddelen moet direct worden gemeld bij de directie of voorzitter van het bestuur.

Artikel 5. Controle
5.1 Controle op gebruik van elektronische informatie- en communicatiemiddelen vindt slechts plaats in het kader van de in artikel 1.2 en 1.3 genoemde doelen.
5.2 De directie 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 in beginsel steekproefsgewijs plaats.
5.5 Als een lid van de directie of de systeembeheerder 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 directie, bestuursleden, vertrouwenspersonen en andere personeelsleden met een vertrouwensfunctie, gecommuniceerd in het kader van hun functie, zijn in beginsel uitgesloten van controle. Dit geldt niet voor de controle bij een ernstig vermoeden van misbruik.
5.7 Er vindt een steekproefsgewijze controle per locatie plaats van het elektronische informatie- en communicatiemiddelenverkeer.
5.8 De geanonimiseerde rapportage wordt verstrekt aan de directie en aan de systeembeheerder. De directie kan naar aanleiding van deze rapportage vragen om een gepersonaliseerde rapportage.
5.9 Indien een personeelslid of een groep personeelsleden ervan wordt verdacht de regels te overtreden, kan gedurende een vastgestelde (korte) periode gerichte controle plaatsvinden. De directie meldt dit aan het bestuur.
5.10 Het bestuur geeft indien nodig aan de systeembeheerder de opdracht om de elektronische informatie- en communicatiemiddelenacties van de betrokkene na te gaan.
5.11 De systeembeheerder brengt hiervan schriftelijk verslag uit aan het bestuur.
5.12 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.
5.13 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 de datum die op het voorblad staat vermeld

Paragraaf 5. 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 Stichting (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 Besturenraad, Bond KBO en Bond KBVO, 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 een computer tot zijn/haar beschikking heeft (dus ook vrijwilligers, stagiaires, enz.). De tekst van de modelregeling sluit op dat punt aan bij de Wet Bescherming Persoonsgegevens (Wbp).

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. Meer informatie over het gebruik van persoonsgegevens is te vinden in het Privacy reglement persoonsgegevens. Een IP-adres is in principe te herleiden tot een bepaalde gebruiker. De tekst van de Wbp is te vinden op: http://wetten.overheid.nl/BWBR0011468
Een specifieke brochure over internetgebruik op de werkplek is bij het College Bescherming Persoonsgegevens op te vragen:
http://www.cbpweb.nl/Pages/av_21_Goed_werken_in_netwerken.aspx

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 stichting).
Gebaseerd op dit artikel kan de stichting (werkgever) overgaan tot het reguleren en controleren van e-mail en internet. Veel werkgevers kiezen ervoor een reglement op te stellen waarin afspraken zwart op wit worden gezet over met name internet en e-mailgebruik. De stichting (werkgever) en het personeel hebben dan schriftelijke afspraken waarin duidelijk staat wat wel en wat niet kan. Op deze manier kan de stichting (werkgever) een inschatting maken tot hoever hij kan gaan met het maken van inbreuken op de privacy van personeel. Laatstgenoemden hebben dan een richtlijn voor de manier waarop ze internet en e-mail dienen te gebruiken.
Uit rechterlijke uitspraken[1] 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. Het is voor werkgevers dan ook veiliger om een duidelijk beleid te hebben. Echter de afwezigheid van een

[1] Kantonrechter Utrecht, 13 juli 2000, JAR 2000, 199; Kantonrechter Apeldoorn, 6 september 2000, JAR 2000, 212; Kantonrechter Utrecht, 20 november 2000, JAR 2001, 7; Kantonrechter Emmen, 29 november 2000, JAR 2001, 4; http://www.cbpweb.nl/downloads_av/av21.pdf.

dergelijk beleid is nog geen rechtvaardiging voor de handelwijze van betrokken werknemers. Ook zonder expliciete gedragscode kunnen werknemers weten wat wel of niet acceptabel is.
Het is van belang te zorgen 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 personeelsnieuwsbrief, 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.

Paragraaf 6. Artikelsgewijze toelichting

Artikel 1. Doel van deze regeling
Deze regeling is van toepassing op personen in dienst van of werkzaam voor de Stichting: 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 stichting 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. Zie hiervoor het Privacyreglement persoonsgegevens. Als er bijvoorbeeld naar aanleiding van een controle reden is om met een personeelslid in gesprek te treden, een waarschuwing te geven, etc. , dan zal dit uiteraard in het personeelsdossier worden vastgelegd (zie ook artikel 5).

Lid 4. In deze regeling is gekozen voor het algemene begrip systeembeheerder. In het basisonderwijs wordt veelal de omschrijving ICT-coördinator of ICT-er gehanteerd. Kenmerkend voor een school in het voortgezet onderwijs is dat er vaak meerdere systeembeheerders ten behoeve van de school werkzaamheden verrichten. In deze regeling is ervoor gekozen de systeembeheerder enkel een technische, signalerende verantwoordelijkheid toe te delen. Daarmee kan voorkomen worden dat een systeembeheerder in een loyaliteitsconflict komt met één van zijn collega's. Bij een vermoeden van misbruik van de EIC-middelen van de Stichting wordt het desbetreffende personeelslid door of namens het bestuur hierop gewezen (zie ook artikel 5.5. van de regeling). Het verdient aanbeveling deze taak niet te mandateren aan de systeembeheerder. Het beheer van de bewakingscamera's is veelal geen taak van de systeembeheerder, maar van de conciërges. Daarom worden ook andere functionarissen beschreven.

Omdat een systeembeheerder 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 systeembeheerder moet tegenover de locatiedirecteur of het bestuur een zekere onafhankelijkheid hebben. Hij mag niet door de locatiedirecteur 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 totaalverbod op het privégebruik van elektronische informatie- en communicatiemiddelen zoals het versturen en ontvangen van persoonlijke e-mailberichten is niet reëel. De Stichting kan wel beperkende voorwaarden stellen aan het privégebruik.

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

- een correcte vermelding van de afzender;
- het meesturen van een disclaimer;
- een duidelijke aanduiding van het onderwerp;
- het 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), dan neemt het bevoegd gezag contact op met de politie. Hiertoe wordt de e-mail uitgeprint en een (digitale) kopie bewaard als potentieel bewijsmateriaal. (NB: 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 regeling. 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 Stichting (werkgever) immers geen arbeidsrelatie waarin hij zijn gezag kan uitoefenen. Zijn positie is in deze situatie vergelijkbaar met een provider.

Het is van belang personeel te adviseren om niet te antwoorden op junk mail, antwoorden op junk mail kan namelijk leiden tot meer junk mail. Adviezen voor het persooneel zijn: 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 onderwerp titels die niets zeggen. Verwijder ieder 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 stichting en het personeelslid. Voor de stichting 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 stichting (werkgever). Hierbij geldt wel dat zij een aantoonbare belangenafweging moet maken tussen haar 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.
Daarnaast zijn er bepaalde doelen 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 van 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/zij 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. Ten slotte kan het personeelslid tegen de verwerking van zijn persoonsgegevens verzet aantekenen in verband met zijn bijzondere persoonlijke omstandigheden.

Lid 9
Als er een vermoeden is op grond waarvan een gepersonaliseerde controle plaatsvindt, wordt het bestuur ingeschakeld. Zie ook de toelichting bij artikel 2 lid 3.
Ook al zou de Stichting niet beschikken over gedragsregels ten aanzien van het gebruik van elektronische- informatie- en communicatiemiddelen, dan mag desalniettemin van het personeel worden verwacht dat het weet 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. Het zal voor een school als werkgever echter verstandig zijn om een duidelijk beleid te voeren. De aanwezigheid van een expliciete regeling zal waarschijnlijk als relevante factor meewegen in een eventuele ontslagprocedure[2].

[2] Kantonrechter Utrecht, 13 juli 2000, JAR 2000, 199; Kantonrechter Apeldoorn, 6 september 2000, JAR 2000, 212; Kantonrechter Utrecht, 20 november 2000, JAR 2001, 7; Kantonrechter Emmen, 29 november 2000, JAR 2001, 4; http://www.cbpweb.nl/downloads_av/av21.pdf.

Referenties

http://www.cbpweb.nl/
College bescherming persoonsgegevens

http://wetten.overheid.nl/BWBR0011468
Wet bescherming persoonsgegevens

http://www.besafeonline.org/dutch/introductie_veilig_internetgebruik.htm
Goede introductie over veilig internetgebruik met allerlei tips

http://www.kennisnet.nl/
Actuele informatie, handreikingen en links over veilig internetten en computerbeveiliging voor ouders, leraren, kinderen, scholieren, schoolmanagers en ICT-coördinatoren van het SURFnet/Kennisnet project.

http://computerbeveiliging.pagina.nl/

http://www.waarschuwingsdienst.nl/

http://www.cbpweb.nl/downloads_av/av21.pdf
Regels voor controle op e-mail en internet gebruik van werknemers door het CBP.

Verklarende woordenlijst

Aanbieder (ISP/Internet Service Provider): bedrijf dat de toegang tot het internet aanbiedt, bijvoorbeeld Xs4all, Chello, en Planet. Letterlijk: verschaffer of verlener.
Attachment (bijlage): letterlijk toevoeging; een bestand dat wordt gekoppeld aan een e-mailbericht. De aanwezigheid van een attachment is zichtbaar door een paperclipsymbool naast het bericht.
Babbelbox: ontmoetingsplaats voor mensen die met behulp van elektronische middelen met elkaar communiceren. Ook wel chatbox genoemd.
Browser: afkorting voor Web Browser. Dit is het programma dat de gebruiker in staat stelt over het web te 'surfen'. De populairste webbrowsers zijn Netscape Navigator en Internet Explorer.
Cache: extra, snel aanspreekbaar geheugen, bedoeld voor het opslaan van veelgebruikte computeropdrachten, waardoor ze sneller beschikbaar zijn.
Chatbox: ontmoetingsplaats voor mensen die met behulp van elektronische middelen met elkaar communiceren. Ook wel babbelbox genoemd.
Chatroom: plekken op internet waar mensen naartoe gaan om met anderen te kletsen ('chatten') in een virtuele kamer. Deze kamers zijn over het algemeen ingedeeld per onderwerp, zodat iedere gebruiker kan kletsen met iemand die dezelfde interesse deelt. Als men zich in een chatroom bevindt, kan men alle gesprekken die plaatsvinden in één keer op het scherm zien.
Cookie: een klein tekstbestand dat door sommige sites op de harde schijf van de pc wordt gezet. Het bevat door de gebruiker opgegeven informatie, zoals voorkeuren of e-mailadres. Als men de site later weer bezoekt, hoeft men niet weer dezelfde vragen te beantwoorden. Het bestand kan gebruikt worden om de gebruiker te volgen en surfgedrag bij te houden op het Web.
Datalimiet: maximale hoeveelheid data die gedownload mag worden.
Disclaimer: letterlijk uitsluiting van verantwoordelijkheid. Disclaimers verschijnen vaak onderaan e-mailberichten of webpagina's. Hierin wordt de lezer erop geattendeerd dat aan de uitspraken geen rechten ontleend kunnen worden.
Domeinnaam: de tekst waarmee een specifieke (internet-)host wordt aangeduid. Domeinen zijn grote gebieden die per doel of soort organisatie verdeeld worden (.com voor commercie, .edu voor onderwijs, gov. voor overheid, org. Voor non-profit, enzovoort).
Download: gegevenstransport van het internet naar een computer. Ook gegevenstransport tussen computer en printer of tussen twee computers.
E-mail: elektronische post. Het stelt de gebruiker in staat berichten over het internet te versturen en te ontvangen.
E-zine: electronic magazine, tijdschrift in elektronische vorm, dat verspreid wordt via e-mail.
Fair Use Policy: de afspraak met een provider dat geen excessief gebruik gemaakt wordt van de verbinding.
FAQ: afkorting van Frequently Asked Questions, hetzelfde als Veel Gestelde Vragen. Om niet telkens alle vragen te hoeven beantwoorden, worden veel voorkomende vragen en bijbehorende antwoorden in een apart bestand gezet.
Favorieten: ook wel bookmarks genoemd. Dit zijn opgeslagen verwijzingen naar websites. Ze stellen de gebruiker in staat zonder omwegen terug te keren naar iedere site, zonder het adres opnieuw in te hoeven typen.
Filteren: hardware of software, ontworpen om bepaalde informatie, zoals porno, geweld en racisme te blokkeren.

Firewall: veiligheidsvoorziening. Bij het kopiëren van bestanden van een andere computer naar de eigen computer kunnen ook virussen binnengehaald worden. Om dat te voorkomen is een firewall een beschermingsmogelijkheid. Het is een beveiliging tussen het externe (internet) en het interne netwerk (LAN), die probeert te voorkomen dat onbevoegden toegang krijgen tot het interne netwerk. Men kan wel van binnen naar buiten gaan, maar niet andersom.
Freeware: gratis software die van internet afgehaald kan worden en die gebruikt mag worden, mits er niets aan veranderd wordt. Er rust copyright op. De software mag niet commercieel verhandeld worden.
FTP: afkorting van File Transfer Protocol, het meest gebruikte standaardprotocol om bestanden te versturen of te ontvangen. Het bestand kan software, tekst, beeld, video of geluid zijn. Na het opgeven van naam en wachtwoord kunnen bestanden verstuurd (upload) worden of ontvangen (download) worden.
Gebruikersnaam: de naam waarmee men zich op internet meldt. Ook wel username of login genoemd.
Hacken: term gebruikt voor het inbreken in computers en computernetwerkendoor het kraken van beveiligingen om aan te tonen dat computers nog lang niet veilig zijn. Hackers proberen via internet netwerken binnen te dringen.
Hoax: een hoax (spreek uit: hooks) is een internetterm voor een loze of valse waarschuwing of een verzonnen verhaal over virussen en trojan horses. Eindeloos verspreid door goedbedoelende internetgebruikers, waardoor een hoax zich min of meer hetzelfde gedraagt als een virus.
Host: letterlijk gastheer. Een host is een centrale computer die grote hoeveelheden gegevens bevat die door meerdere terminals kunnen worden benaderd. De host is door vaste lijnen te koppelen aan terminals, maar kan ook gekoppeld worden aan computers via tijdelijke verbindingen ('server') waarop een website fysiek is gelokaliseerd.
HTML: afkorting voor HyperText Mark-up Language. HTML is de programmeertaal waardoor het internet werkt. HTML is een zogenaamde onderscheidingstaal. Het heeft de taak de bestanddelen van een document te beschrijven. HTML bevat opdrachten voor het markeren van document-elementen, zoals kopteksten, tekstgedeeltes, lijsten, tabellen of grafische referenties, uitgaande van een hiërarchische deling.
Hyperlink: een link zorgt ervoor dat men met slechts één muisklik van de ene naar de andere internetsite gaat. Links kunnen bestaan uit een tekst of een afbeelding. Tekstlinks zijn meestal onderstreept en hebben vaak een kleur die afwijkt van de rest van de tekst. Afbeeldinglinks kunnen plaatjes, tekeningen of animaties zijn. Op een link verandert de muisaanwijzer meestal in een handje. De link is in feite het internetadres waarheen verwezen wordt.
ICQ: kort voor I Seek You - ik zoek je. Programma dat gebruikt kan worden om te kijken of er bekenden online zijn. Zij moeten dan ook ICQ gebruiken.
ICT: afkorting van Informatie- en CommunicatieTechnologie. Gebruikt voor alles wat te maken heeft met automatisering en telecommunicatie.
IP: afkorting van Internet Protocol. De op internet gehanteerde taal om gegevens uit te wisselen. Met deze taal kan een computer precies aangeven naar welk adres de informatie toe moet.
IRC: afkorting van Internet Relay Chat. IRC is voor internetgebruikers een manier om met elkaar over allerlei onderwerpen te praten. Oneerbiedig wordt IRC ook wel de babbelbox van internet genoemd. Soms zijn de discussies door iedereen te volgen, soms niet. De gesprekken zijn altijd realtime. Dat wil zeggen, voor de één kan het zeven uur 's morgens, voor de ander kan het twee uur 's nachts zijn. Het

is een van de populairste toepassingen van internet. Ook is er een heel apart jargon ontstaan bij IRC'ers.
ISP: afkorting van Internet Service Provider. Organisatie die via eigen servers andere organisaties en privé-gebruikers toegang biedt tot internet.
LAN: afkorting van Local Area Network, computernetwerk binnen een beperkt gebied, bijvoorbeeld binnen een gebouw of een universiteitscomplex. De aangesloten gebruikers delen ook printers en andere apparatuur.
Modem: modems zorgen ervoor dat informatie van de ene computer naar de andere kan worden overgedragen via elke telefoonlijn.
Nieuwsgroepen: dit zijn elektronische discussiegroepen voor mensen op het Internet die een interesse delen. Ze zijn vergelijkbaar met chatrooms, behalve dat de berichten niet verschijnen op het moment dat ze worden geschreven en dat meer mensen er toegang tot hebben.
Online: rechtstreeks via bijvoorbeeld een telefoonlijn in verbinding staan met een andere computer. Dat kan met een provider zijn en daardoor met internet.
Provider: zie aanbieder.
Server: een machine die de zware klussen afhandelt zoals het sorteren en versturen van e-mail, het onderhouden van sites en het aanbieden van websites aan klanten.
SPAM: de internetversie van 'junk e-mail'. 'Spamming' betekent hetzelfde bericht versturen aan een grote hoeveelheid gebruikers. Meestal gaat het om advertenties.
Startpagina (homepage): 1. de voornaamste pagina van een website, de voordeur. 2. iemands persoonlijke pagina op het Web. 3. de pagina waarmee een web browser opent. 4. Naam van een handige website met gerubriceerde onderwerpen.
Trojan horse: ook wel Trojaans paard: een onschuldig ogend computerprogramma met kwade bedoelingen. Het doet zich voor als een bruikbaar stuk software, maar - eenmaal genesteld in de computer van het slachtoffer – stuurt het vertrouwelijke informatie naar de maker ervan.
Update: verbetering van een softwareprogramma. Een update wordt vaak gebruikt voor de modernisering van een programma.
USB: afkorting van Universal Serial Bus. Nieuwe standaard voor het aansluiten van allerlei zeer uiteenlopende apparatuur.
URL: afkorting van Uniform Resource Locator. Dit is een onderdeel van een Internetadres dat wordt weergegeven in een vorm die voor iedere web browser begrijpelijk is. Het is een standaard soort adres voor ieder bestand, voorwerp of bron op het Internet. Het adres van een website begint met http://.
Upload: bestanden van een eigen computer naar een andere computer kopiëren. Dat kan een computerprogramma, tekst, beeld of geluid zijn. Het tegenovergestelde van uploaden is downloaden.
Virus: een computervirus kan informatie op uw computer uitwissen en grote problemen veroorzaken.
Wereld Wijde Web (World Wide Web): het Web is een universele verzameling van webpagina's, die door hyperlinks met elkaar worden verbonden.
Zoekmachine (search engine): een grote gegevensbank van internetadressen. Internetgebruikers kunnen deze op het Web bezoeken om vragen te stellen over hun zoektocht. Bekende zoekmachines zijn Ilse, Google, Yahoo en Altavista.