PROTOCOL voor het gebruik van

Elektronische Informatie- en Communicatiemiddelen (EIC)

bij De Haagse Scholen, stichting voor primair en speciaal openbaar onderwijs.

Vastgesteld door het Centraal Directie Overleg van De Haagse Scholen, stichting voor primair en speciaal openbaar onderwijs, op 3 maart 2010.

Artikel 1 Doel en werkingssfeer van dit protocol

1.1 Dit protocol geeft de wijze aan waarop bij De Haagse Scholen, stichting voor primair en speciaal openbaar onderwijs (DHS), wordt omgegaan met (elektronische) informatie- en communicatiemiddelen. Dit protocol omvat gedragsregels ten aanzien van verantwoord gebruik.

1.2 Onverantwoord gebruik is gebruik tegenstrijdig aan de doelstelling en identiteit van de scholen, inclusief het bestuurskantoor, van De Haagse Scholen, zowel in persoonlijk gebruik als in relatie tot anderen binnen of buiten de school, inclusief het bestuurskantoor. Hierbij wordt in het bijzonder gedacht aan illegale toepassingen van bestanden, godslasterlijke, beledigende, aanstootgevende, gewelddadige, racistische, discriminerende, intimiderende, seksueel getinte toepassingen, zinloos tijdverdrijf en/of toepassingen die strijdig zijn met de wet of als onethisch te karakteriseren zijn.

1.3 Dit protocol geldt voor een ieder die werkzaam is bij en ten behoeve van de school c.q. het bestuurskantoor. Het onderwijspersoneel ziet er op toe dat ook de leerlingen van De Haagse Scholen handelen overeenkomstig de bepalingen van dit protocol.

Artikel 2 Gebruik van informatie- en communicatiemiddelen

2.1 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 c.q. DHS, het verzenden van post als ook voor wat betreft het gebruik van (elektronische) informatie- en communicatiemiddelen. Voorbeelden van deze middelen zijn: papier, (mobiele) telefoon, cd, dvd, usb-stick, pda, mp3 speler, camera, smartphone, mail, chat, pc's, laptops etc.

2.2 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 protocol.

2.3 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. Men is zelf verantwoordelijk voor de apparatuur waarvan gebruik wordt gemaakt. Laat deze in actieve stand niet onbeheerd achter. Actieve sessies moeten bij het verlaten van de werkplek worden beëindigd. Op die manier kunnen anderen niet van bevoegdheden gebruik maken.

2.4 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 werkgerelateerd dagboek en het bezoeken van chatboxen.

2.5 Het is in het bijzonder niet toegestaan om:

- bewust sites te bezoeken die seksueel getint, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten;
- bewust seksueel getint, 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;
- anders dan om professionele redenen computerspelletjes 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;
- inkomende privé-berichten te genereren door het deelnemen aan niet-zakelijke nieuwsgroepen, elektronisch winkelen, down- en uploaden van bestanden, nieuwsbrieven en dergelijke;
- kettingmailberichten te verzenden of door te sturen;
- een mobiele telefoon van de school / het bestuurskantoor te gebruiken in het buitenland zonder uitdrukkelijke toestemming van het bevoegd gezag;
- iemand lastig te vallen.

2.6 Het is niet toegestaan om individueel belastende / privacy gevoelige foto's, video's of ander materiaal van op school c.q. bij DHS werkzame personen of leerlingen of andere bij de school c.q. DHS betrokkenen via elektronische informatie- en communicatiemiddelen bekend te maken.

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

2.8 User-identifcatie (gebruikersnaam) en authenticatie (bijvoorbeeld wachtwoord) zijn strikt persoonsgebonden en mogen niet aan anderen worden doorgegeven. Wanneer het vermoeden bestaat dat anderen het wachtwoord kennen, dient men het wachtwoord te wijzigen.

2.9 Onbedoelde inbreuken op beveiliging, van binnenuit of van buiten de school c.q. DHS dienen onmiddellijk aan de systeembeheerder (ICT-sectie) van De Haagse Scholen gemeld te worden.

Artikel 3 Meldingsplicht

Een vermoeden van misbruik van (elektronische) informatie- en communicatiemiddelen moet direct worden gemeld bij de schoolleiding of de centrale directie van DHS.

Artikel 4 Controle

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

4.2 De centrale directie respectievelijk de schoolleiding informeert in voorkomende gevallen de personeelsleden over controle op (elektronische) informatie- en communicatiemiddelen, omtrent de doeleinden, de aard van de gegevens en de omstandigheden waaronder zij verkregen zijn. Dit informeren kan vooraf gedaan worden, met name als preventief middel, en anders achteraf.

4.3 Niet toegestaan gebruik van (elektronische) informatie- en communicatiemiddelen (EIC) wordt zo veel mogelijk technisch onmogelijk gemaakt.

4.5 Als een lid van de centrale directie respectievelijk de schoolleiding of de systeembeheerder / ICT-sectie van De Haagse Scholen 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.

4.6 (Elektronische) informatie- en communicatieberichten van de schoolleiding, centrale 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.

4.7 Indien een personeelslid of een groep personeelsleden ervan wordt verdacht de regels te overtreden, kan gedurende een vastgestelde (korte) periode gerichte controle plaatsvinden. De schoolleiding meldt dit, vooraf dan wel achteraf, aan de centrale directie.

4.8 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.

4.9 Bij handelen in strijd met deze regeling beslist de centrale directie respectievelijk het bestuur (waar het gaat om leden van de centrale directie), over de al dan niet te nemen (disciplinaire) maatregelen. Tot deze maatregelen kan ontslag uit het dienstverband behoren.

Artikel 5 Inwerkingtreding en citeertitel

Dit protocol treedt in werking per 8 maart 2010 en kan aangehaald worden als 'Informatie- en communicatieprotocol van De Haagse Scholen 2010'.

Toelichting op het protocol

Dit protocol betreft het gebruik van informatie- en communicatiemiddelen zoals deze ter beschikking zijn/worden gesteld of worden gefinancierd door de school c.q. DHS (als werkgever).

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

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 c.q. de organisatie van DHS).
Gebaseerd op dit artikel kan de school / DHS (werkgever) overgaan tot het reguleren en controleren van e-mail en internet. Veel scholen / organisaties kiezen ervoor een reglement op te stellen waarin afspraken zwart op wit worden gezet over met name internet en e-mailgebruik. De school c.q. DHS (werkgever) en het personeel hebben dan schriftelijke afspraken waarin duidelijk staat wat wel en wat niet kan. Op deze manier kan de school c.q. DHS (werkgever) een inschatting maken tot hoever hij gaan kan met het maken van inbreuken op de privacy van op school c.q. bij DHS 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 c.q. bij DHS 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, plaatsing op het intranet van De Haagse Scholen, bij het uitreiken van een e-mailadres of een nieuwe mobiele telefoon e.d.

Artikelsgewijze toelichting

Artikel 1 Doel van dit protocol

Dit protocol is van toepassing op personen in dienst van of werkzaam voor de school c.q. DHS: 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 c.q. DHS 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 c.q. DHS verrichten.

Artikel 2 Gebruik van (elektronische) informatie- en communicatiemiddelen (EIC)

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 c.q. DHS kan wel beperkende voorwaarden stellen aan het privégebruik.

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.

Het personeel wordt geadviseerd 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.

Artikel 4 Controle

Het gebruik van (elektronische) informatie- en communicatiemiddelen leidt per verschijningsvorm tot andere risico's voor de school c.q. DHS en het personeelslid. Voor de school c.q. DHS 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 c.q. DHS (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 c.q. DHS 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 dient 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 en vloeit ook voort uit de Arbowetgeving.

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 bij de algemeen directeur van De Haagse Scholen, in verband met zijn bijzondere persoonlijke omstandigheden.

Artikel 4 lid 9

Als er een vermoeden is op grond waarvan een gepersonaliseerde controle plaatsvindt, wordt de centrale directie respectievelijk het bestuur van De Haagse Scholen ingeschakeld.