Protocol cyberpesten en mediawijsheid OPSO en SPOOR

-2014

Status:

Datum	Geleding	Naam
Juni 2014	Steller	M. Selij/G. Stavenuiter
Oktober 2014	Projectgroepen	H. Plaatsman / H. Oudega
September 2014	Directeurenoverleg	Alle directeuren OPSO/SPOOR
17 maart 2015	GMR	N. Bonenkamp / A. Laverman
December 2014	College van Bestuur	A. Kuiper / J. de Graaf
	Raad van Toezicht	S. van Geldorp / P. Tange

Gebruikte documenten voor de aanpassing het protocol cyberpesten en mediawijsheid OPSO/SPOOR:

- Protocol mediawijsheid SPOOR
- Internetprotocol op school (de AVS)
- Positief Social media Protocol (Social media wijs)
- Afspraken voor alle scholen binnen de stichting over het gebruik van internet

VOORWOORD

Deze gedragscode “Mediawijs” geldt voor de medewerkers en de leerlingen van OPSO en SPOOR. Dit protocol sluit aan op de hedendaagse gemedialiseerde sociale wereld. De medewerkers en leerlingen die gebruik maken van de nieuwe media worden via dit protocol op de hoogte gebracht van wat is toegestaan en wat niet. In dit protocol leggen we m.b.t. het gebruik van multimedia het gewenste gedrag van leerlingen en medewerkers vast.
De gedragscode “Cyberpesten en Mediawijs’ is met ingang van 2015 van kracht. Vanaf dat moment is de versie uit 2010 niet meer van toepassing en kan daar ook niet meer naar verwezen worden.

Inhoudsopgave **pag.**

INLEIDING

'Mediawijsheid', iedereen moet mediawijzer worden.

Maar wat betekent nu eigenlijk 'mediawijs(heid)'.

De definitie van de Raad voor Cultuur in hun advies in 2005 luidde:

'Mediawijsheid staat voor het geheel van kennis, vaardigheden en mentaliteit waarmee burgers zich bewust, kritisch en actief kunnen bewegen in een complexe, veranderlijke en fundamenteel gemedialiseerde wereld'.

Het gaat er om, dat we in staat zijn oude en nieuwe media (internet toepassingen w.o. chatten) te gebruiken en dat we een gezonde mentaliteit ten opzichte van deze media hebben, waarbij we ons bewust zijn van de mogelijkheden en van de context van informatie. De vaardigheden met betrekking tot nieuwe media kunnen worden ingedeeld in:

- ICT vaardigheden
- Informatievaardigheden
- Veilig mediagebruik

Ook voor onze basisschoolleerlingen is het gebruik van o.a. de mobiele telefoon, internet, e-mail en de daarbij behorende sociale netwerken, zoals o.a. msn, facebook en twitter worden steeds meer gebruikt.

Binnen het bestuur OPSO/SPOOR zijn afspraken gemaakt over het gebruik van Multi Media. De afspraken zijn uitgewerkt in het protocol 'Cyberpesten en Mediawijs'.

<u>Uitgangspunten:</u>

- Onze scholen hebben de mogelijkheid via QLICT een content filter te gebruiken. Dit content filter kan via een white- en blacklist door de school worden aangepast. De school bepaalt zelf of content filtering wordt toegepast. In acht moet worden genomen dat content filtering nooit voor 100 % werkt.
- Alle groepen, leerkrachten en overige gebruikers maken gebruik van e-mail. Wanneer er een mailbox voor de groep is aangemaakt dan beheert de groepsleerkracht deze en is verantwoordelijk voor de inkomende - en uitgaande mail.
- Het wel of niet meenemen van eigen mobile devices door leerlingen naar school (GSM, Tablet, Smartwatch en hetgeen op korte termijn nog meer wordt uitgevonden) verschilt per school. Een aantal scholen zullen in de zeer nabije toekomst kiezen voor BYOD (bring your own device). Regels hierover zullen in de schoolgids moeten worden vastgelegd. Scholen die overstappen op BYOD of op een andere manier met mobile devices gaan werken, wordt sterk aangeraden gebruik te maken van een MDM (Mobile device manager). Hiermee kan de school exact bepalen wat leerlingen binnen de school met deze devices kunnen en mogen doen. Het meenemen van mobile devices is alleen toegestaan na toestemming van de leerkracht, binnen de regels van de school en is op eigen risico.
- Het veilig gebruik maken van Social media zal middels media lessen aan de orde komen.

1. INTERNET / E-MAIL

1.1 Algemeen

Personeelsleden en leerlingen moeten in staat zijn met behulp van internet informatie te zoeken, te verwerken en uit te wisselen. Daarbij wordt binnen de school de strategie toegepast van 'begeleidend confronteren', **je leert kinderen omgaan met internet zoals het is!** Internet is een afspiegeling van de maatschappij. Net als in de maatschappij moeten kinderen leren wat goed is en wat niet goed is, wat kan en wat niet kan. Zoals je leert kinderen om te gaan met de televisie en druk verkeer, zo moet dat ook met het internet: onder begeleiding stapje voor stapje de wereld van het internet eigen maken. Bespreek met de

kinderen de gevaren/risico's, maar vooral ook de voordelen van internet.

1.2 Enkele voordelen

- Personeelsleden en leerlingen kunnen van het internet gebruik maken als onderdeel van het onderwijs: om informatie te zoeken, contacten te leggen met leerlingen van andere scholen en deskundigen te kunnen raadplegen;
- Software die voor het onderwijs wordt ontwikkeld, verwijst meer en meer naar internetsites voor aanvullend, actueel of alternatief materiaal. Internetactiviteiten worden hiermee steeds meer onderdeel van methodes en leergangen. De educatieve multimediale software die bij bepaalde methodes hoort, kan in de toekomst door leerlingen ook via internet benaderd worden.

1.3 Enkele risico's

- Niet alles op internet is geschikt voor onze doelgroep. Ongewenst is niet alleen pornografie, maar ook teksten of afbeeldingen die betrekking hebben op bijvoorbeeld extreem geweld, racisme of extremisme;
- Sommige websites hebben een onvolledige, misleidende of foutieve inhoud;
- Wanneer kinderen persoonlijke informatie doorgeven via sociale netwerken en e-mail, kan dit leiden tot schadelijke contacten. Pedofielen doen zich bijvoorbeeld op het internet soms voor als kinderen en proberen afspraakjes in de echte wereld te maken;
- Als je een bericht stuurt naar een nieuwsgroep of een bedrijf kan het gevolg zijn, dat je heel veel ongewenste reclame (Spam) in je elektronische brievenbus (Inbox) krijgt;
- Door het min of meer anonieme karakter van het internet lokt het medium, met name bij sociale netwerken (Instagram, Facebook, MSN enz.) en e-mail, uit tot het gebruik van grof of kwetsend taalgebruik.
- Het verspreiden van auteursrechtelijk beschermd materiaal op internet is zonder toestemming van de gerechtigde niet toegestaan;
- Ook virussen kunnen via internet binnenkomen. Met name de e-mail virussen vormen een groot risico;
- Inbreken op de computer (hacken) door kwaadwilligen is een toenemend risico.
- Het gebruik van social media gebeurt 'real time'. Een druk op de knop en jouw bericht staat direct online;
- Online informatie kan een lange periode online staan. Het is niet altijd gemakkelijk om informatie naderhand te (laten) verwijderen;
- Het is geen oplossing om eenmaal geplaatste berichten zomaar te verwijderen.
- Met een druk op de knop (real time) worden ook foute berichten online geplaatst.

1.4 Gebruikersvoorwaarden

- Leerlingen worden goed begeleid; zij worden door de leerkrachten gewezen op welke manieren zij informatie kunnen zoeken, verwerken en uitwisselen;
- Leerkrachten, leerlingen en ouders zijn zich bewust van de risico's van internet;
- De leerkrachten volgen de verrichtingen van de leerlingen op internet;
- Ook wordt in bepaalde gevallen (vermoeden van misbruik) via de adresbalk van 'Internet Explorer', bij 'Geschiedenis' of de 'Verkenner' in de mappen 'Windows/Cookies' en 'Windows/Temporary internet files' controle uitgeoefend.
- De netwerkomgeving is beveiligd middels een firewall. Deze firewall wordt beheerd door QLICT. Het internet kan worden beveiligd middels een content filter. De school bepaalt of het content filter wel of niet wordt gebruikt. Het bijhouden van de black en white list van het content filter wordt gedaan door QLICT maar kan door de school zelf worden aangepast. De veiligheid van het netwerk en daarmee het internet valt en staat bij een goed wachtwoord beleid. Wachtwoorden zijn vergelijkbaar met je pincode en zijn absoluut persoonlijk. Deel nooit je wachtwoord met een ander en bij het vermoeden dat het wachtwoord bekend is, dit direct wijzigen. Alle servers van onze scholen en de (toekomstige) cloud opslag is op afstand te benaderen. De enige beveiliging tegen misbruik is een goed wachtwoord.
- Er worden door de gebruikers geen internetsites bezocht die obscene, tot haat opruiende of anderszins aanstootgevende informatie bevatten.

- Het “Pestprotocol” maakt geen onderscheid tussen pesten en Cyberpesten. Onder cyberpesten verstaan we het verzenden of ontvangen van obscene of lasterlijke informatie of informatie die tot doel heeft andere personen te ergeren, kwellen of intimideren;
- De werking van het Internet wordt niet opzettelijk verstoord, waaronder ook wordt verstaan het verspreiden van computervirussen of netwerkverkeer van grote omvang over langere tijd, waardoor anderen wezenlijk worden gehinderd bij hun gebruik van het internet (w.o. elektronische kettingbrieven, het downloaden van grote bestande, het luisteren naar internet radio of het niet werk gerelateerd bekijken van streaming video.);
- Internet en E-mail worden niet gebruikt voor onwettige activiteiten;
- Er worden geen ontoelaatbare opmerkingen, voorstellen of materialen op het Internet geplaatst;
- Het uploaden, downloaden of anderszins overbrengen van commerciële software of materiaal waarop rechten van derden rusten, zoals auteursrechten, wordt niet als legaal gebruik gezien;
- Software of computerbestanden van internet worden niet opgehaald en/of geïnstalleerd zonder de maatregelen voor bescherming tegen virussen te nemen die door het schoolbestuur en de directie van de school zijn voorgeschreven;
- Vertrouwelijke informatie of informatie die eigendom is van personen of instellingen worden niet bekend gemaakt of gepubliceerd. Dergelijke informatie bestaat onder meer uit, maar niet beperkt tot: databases van het schoolbestuur of de school en de daarin opgeslagen gegevens, computersoftware, toegangscodes voor computernetwerken en persoonlijke gegevens van leerlingen van de school;
- Er worden geen bestanden, van andere personen geopend, gebruikt, of gewijzigd zonder uitdrukkelijke toestemming van die personen;
- Er wordt kortweg niet in strijd gehandeld met wat in het maatschappelijk verkeer betaamt.

1.5 Afspraken leerlingen

- Zonder toestemming van mijn leerkracht mag ik niet op internet;
- In de pauzes mag ik zonder de aanwezigheid van een leerkracht niet op internet;
- Ik geef nooit mijn eigen naam of adres weg, ook niet mijn e-mailadres;
- Ik verstuur per e-mail nooit een foto of filmpje van mijzelf of van anderen zonder toestemming van de leerkracht;
- Chatten mag ik niet op school tenzij dat voor de les wordt vereist en er toestemming is gegeven door de leerkracht.
- Communiceren (mailen, chatten, wordfeud e.d.) met personen buiten de school is tijdens de lessen niet toegestaan tenzij dat voor de les wordt vereist en er toestemming is gegeven door de leerkracht.
- Ik houd mijn wachtwoord(en) voor iedereen geheim. Ik gebruik geen voor de hand liggend wachtwoord (de naam van mijn huisdier, voetbalclub of postcode is door bekenden makkelijk te raden);
- Ik maak geen afspraakjes met mensen die ik alleen ken via internet;
- Ik lees en beantwoord geen e-mails van onbekenden en open zeker geen bijlagen gestuurd door onbekenden (daar kan een virus in zitten); ongewenste figuren die mij mailen of MSN-en blokkeer ik.
- Ik ga direct naar mijn leerkracht als ik op internet informatie over seks, geweld of andere informatie en/of beelden tegenkom waarvan ik denk dat deze beelden niet gepast zijn;
- Ik reageer niet op gemene, valse, vervelende berichten. Het is niet mijn schuld, dat sommige mensen zich niet weten te gedragen. Als het gemene, kwetsende dingen zijn, waarschuw ik direct mijn leerkracht en/of ouders. Zij nemen dan mogelijk contact op met de politie;
- Ik verstuur zelf ook geen gemene, valse, vervelende, kwetsende berichten;
- Ik gebruik internet of e-mail om opdrachten, die ik van mijn leerkracht krijg uit te voeren;
- personeelsleden, leerlingen en ouders gebruiken de multimedia niet om privé contacten met elkaar te onderhouden;

1.6 Afspraken personeelsleden

- Personeelsleden gaan professioneel om met vertrouwelijke informatie vanuit de school;
- Personeelsleden gebruiken internet en hun mobile device uitsluitend professioneel;
- Deze afspraken worden minimaal 1 maal per jaar met de personeelsleden en de leerlingen besproken;
- De regels die uit deze afspraken voorkomen zijn bij elke werkplek te lezen;

- Deze afspraken zijn terug te vinden in de schoolgids en op de website van de school.

1.7 Tips om de eigen privacy te beschermen

- Vraag toestemming aan je ouders als je alleen ergens wilt chatten;
- Gebruik altijd een Nickname tijdens het chatten;
- Geef geen gegevens van jezelf of vrienden aan iemand die je op de chat ontmoet. Dus geen emailadressen, namen (ook niet van school), telefoonnummers enz.;
- Reageer niet op seksuele vragen of op scheldpartijen. Als er iets vervelends gebeurt op de chat, dan ga je weg en informeer je je ouders/verzorgers;
- Bel niet zomaar met kinderen die je van de chat kent, en spreek niet met ze af, zonder dat je ouders/verzorgers dat weten;
- Onbekende mensen verwijder je uit je vriendenlijst;
- Op internet kan je eenvoudig een eigen pagina op een zogenaamde profielsite maken. Leuk om aan al je vrienden te laten zien, maar besef dat de hele wereld jouw profiel kan zien. Denk goed na welke informatie en welke foto's je van jezelf wilt gebruiken. Plaats in ieder geval geen informatie waardoor mensen kunnen herleiden hoe je heet, waar je woont, op welke school je zit, etc.;
- Deze tips zijn terug te vinden in de schoolgids en op de website van de school.

2. **MOBILE DEVICES**

2.1 Mobiel kan alles

De techniek verandert snel. Een telefoon is al lang geen telefoon meer alleen, maar een volwaardige computer en andere mobile device zoals de tablet kunnen worden gebruikt om te telefoneren. Het is daarom goed niet meer van mobiele telefoons te spreken maar van mobile device. De meeste kinderen gebruiken hun mobile device om te bellen, te sms'en, de social media bij te houden, als wekker, horloge, mp3-speler, spelcomputer, internet toegang en fototoestel.
Ook binnen de scholen van OPSO en SPOOR neemt het bezit van de mobiele telefoon toe. Veel ouders willen dat hun kind goed bereikbaar is voor, tijdens en na schooltijd.

2.2 Enkele voordelen

- **Veiligheid:**
  Kinderen zijn voor de ouders altijd bereikbaar.

- **Contact met vrienden (sociale netwerken):**
  Het sociaal netwerken en contact met vrienden, wordt naarmate de kinderen ouder worden belangrijker. Het maken van foto's en filmpjes is eenvoudig en gemakkelijk vast te leggen en door te sturen.

- **Multimediale functies:**
  Bellen, sms'en, whatsapp, horloge, mp3-speler, fototoestel, spelletjes, internet, GPS en Google maps (navigatie).

2.3 Enkele risico's

- **Informatie uitwisselen:**
  Wanneer kinderen persoonlijke informatie doorgeven via sociale netwerken en e-mail, kan dit leiden tot schadelijke contacten. Pedofielen doen zich bijvoorbeeld op het internet soms voor als kinderen en proberen afspraakjes in de echte wereld te maken. Ook cyberpesten ligt op de loer.

- **Foto's:**
  Telefoons met camera's en toegang tot internet brengen gemak met zich mee, maar werken ook pestgedrag in de hand. Kinderen maken filmpjes van zichzelf en van anderen en sturen die door, soms met kwade bedoelingen. Het uploaden, downloaden of anderszins overbrengen van commerciële software of materiaal waarop rechten van derden rusten, zoals

auteursrechten, wordt niet als legaal gebruik gezien.

2.4 Afspraken

- Het gebruik van eigen mobile devices binnen de school verschilt per school. In sommige gevallen zal het gebruik van eigen mobile devices worden verboden. De mobile devices wordt dan ingeleverd bij de leerkracht en is uitgeschakeld.
- Als de school BYOD toepast zal het gebruik van de devices goed in een protocol moeten worden vastgelegd. Het gebruik van een MDM wort aanbevolen.
- In noodgevallen is ieder kind tijdens schooltijd **altijd bereikbaar** onder het vaste nummer van de school;
- Het gebruik van mobile devices door medewerkers kan per school verschillen. Ook voor medewerkers kan het mobile device onderdeel uitmaken van het schoolnetwerk. Essentieel is dat het device tijdens werktijd professioneel en niet privé wordt gebruikt.
- De school / werkgever is niet aansprakelijk voor het wegraken/kapot gaan van de mobile devices.
- Het meenemen van een mobile device is op eigen risico.

3. **OVERTREDEN GEDRAGSCODE**

Bij het overtreden van de gedragscode en de schoolafspraken treedt de volgende procedure in werking.

3.1 Overtreden gedragscode internet en e-mail

- Wanneer er sprake is van cyberpesten, gaat het stappenplan van het pestprotocol in werking.
- Bij minder ernstig misbruik krijgt de betrokken leerling een waarschuwing van de groepsleerkracht. Indien niet tot overeenstemming wordt gekomen, wordt advies aan de directie van de school gevraagd die vervolgens een doorslaggevend advies geeft. De directie stelt de ouders van de betrokken leerling daarvan op de hoogte.
- Bij ernstig misbruik worden de betrokken leerling en de ouders van deze leerling in kennis gesteld door de directie van de school. Daarbij wordt schriftelijk de aard van de overtreding vermeld en - indien dat het geval is - waarom de toegang van de leerling tot Internet wordt geblokkeerd en/of het e-mail adres wordt verwijderd.
- Bij ernstig misbruik wordt de betrokken medewerker in kennis gesteld door de directeur van de school. Daarbij wordt de aard van de overtreding gemeld en schriftelijk vastgelegd. De directeur is verplicht de overtreding door te geven aan het College van Bestuur.
- De ICT-coördinator/systeembeheerder op schoolniveau onderzoekt onmiddellijk iedere melding van mogelijk misbruik en meldt het resultaat vervolgens meteen aan de groepsleerkracht indien het een leerling betreft en aan de directie van de school als het een personeelslid of een andere gebruiker betreft. Onmiddellijk na de melding blokkeert de ICT-coördinator/systeembeheerder het e-mail adres en blokkeert de internettoegang.

3.2 Overtreden gedragscode mobiele telefoon

- Wanneer er sprake is van cyberpesten, gaat het stappenplan van het pestprotocol in werking.
- Bij minder ernstig misbruik krijgt de betrokken leerling een waarschuwing van de leerkracht en wordt de mobiele telefoon ingenomen. Na schooltijd kan de betrokken leerling haar/zijn mobiele telefoon bij de groepsleerkracht ophalen. Indien niet tot overeenstemming wordt gekomen, wordt advies aan de directie van de school gevraagd die vervolgens een doorslaggevend advies geeft.
- Bij ernstig misbruik worden de betrokken leerling en de ouders van de betrokken leerling in kennis gesteld door de directie van de school. Daarbij wordt de aard van de overtreding schriftelijk vermeld en waarom de mobiele telefoon voor onbepaalde tijd is ingenomen. De betrokken ouders kunnen de mobiele telefoon na schooltijd komen ophalen.
- Wanneer een medewerker op enige wijze misbruik maakt van de mobiele telefoon, wordt deze door de directeur hierop aangesproken.
- Bij ernstig misbruik spreekt de directie de medewerker hierop aan. Daarbij wordt de aard van

de overtreding duidelijk gemaakt en schriftelijk vastgelegd. De directie is verplicht deze overtreding te melden bij het College van Bestuur.

4. VEILIGHEIDSGARANTIES

- De school zorgt er voor dat de leerlingen tijdens de lessen geregeld tekst en uitleg krijgen over de voordelen en de risico's van internet-, chat-, e-mailverkeer en de mobile devices.
- De afspraken uit dit protocol en de eventuele schoolafspraken over het eigen gedrag zijn voor de leerlingen in het lokaal duidelijk zichtbaar, opdat zij steeds worden herinnerd aan wat wel en niet toelaatbaar is.
- De gedragscode cyberpesten en mediawijsheid wordt vermeld in de schoolgids en is te lezen op de website van de school.
- Een schriftelijk exemplaar van de gedragscode kan bij de directie worden ingezien.
- In opdracht van het schoolbestuur en de directie is de externe systeembeheerder, QLICT verantwoordelijk voor het onderhoud, het beheer en de controle van de netwerkbeveiliging. De veiligheidseisen worden bovenschools aangestuurd.
- De verantwoordelijkheid voor de veiligheid is verdeeld over drie niveaus:

  Extern: QLICT (externe systeembeheerder van het netwerk) installeert, beheert en onderhoudt de antivirussoftware, de firewall, de spam-filter en de updates van de content filtering en beveiligingssoftware. KPN/XS4ALL, UPC en Ziggo beheren en onderhouden de breedbandverbinding voor internet.

  Schoolniveau: De directie van de school stelt samen met de ICT-coördinator van de school een gedragscode voor gebruikers op en informeert de leerkrachten, de ouders en het schoolbestuur. De ICT-coördinator van de school onderhoudt namens de directie van de school het contact met de externe systeembeheerder over de beveiliging van het netwerk en beheert en onderhoudt de interne beveiliging (o.a. het toekennen van rechten voor gebruikers). De ICT-coördinator scherpt na overleg met de directie waarnodig de gedragscode aan. Aanpassingen zijn altijd onmiddellijk, nadat de gebruikers zijn geïnformeerd, van kracht!

  Bovenschools: het schoolbestuur van OPSO en SPOOR beheert en onderhoudt, in samenwerking met QLICT de mailserver van Office 365. Scholen die geen gebruik maken van Office 365 zijn zelf verantwoordelijk voor het beheer van de mailboxen.. Alle gebruikers binnen de scholen van OPSO en SPOOR w.o. ook de groepen krijgen een school mailadres. De eindverantwoording voor het gebruik van mobile devices, internet, chatten en e-mail binnen school ligt altijd bij het schoolbestuur (OPSO/SPOOR). Het college van bestuur wordt direct van misbruik op de hoogte gesteld wanneer het een directielid of personeelslid aangaat. Betreft het een leerling of een persoon die vanwege zijn/haar activiteiten op school gebruik maakt van internetfaciliteiten en/of e-mail, dan zal in eerste instantie de directie namens het bestuur maatregelen treffen.

Meer informatie over veiligheidskwesties, media-educatie en cyberpesten is te vinden op:

- www.kennisnet.nl
- www.mijnkindonline.nl
- www.mediawijzer.nl
- www.pestenislaf.nl
- www.digitalfilecheck.nl
- www.safer-internet.net (Engelstalig)
- www.pro-music.nl (Engelstalig)
- www.surfsleutel.nl (een wegwijzer voor kinderen op internet)