VOORWOORD

Deze gedragscode “Mediawijs” geldt voor de leerlingen op de scholen van SPOOR. Dit protocol sluit aan op de hedendaagse gemedialiseerde sociale wereld. De leerlingen die de nieuwe media op school gebruiken kunnen weten wat is toegestaan en wat niet. De leerkrachten kunnen op basis van dit protocol nagaan wanneer er sprake is van onveilig gebruik of misbruik van de nieuwe media.
De gedragscode ‘Mediawijs’ (2010) is met ingang van 19 / 04 / 2011 van kracht. Vanaf dat moment is de versie uit 2005 niet meer van toepassing en kan daar ook niet meer naar verwezen worden.

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 (tv, radio, pers) en nieuwe media (internettoepassingen 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, msn, hyves (66% van alle Nederlandse gebruikers van sociale netwerken), facebook (27% van alle Nederlandse gebruikers van sociale netwerken) en twitter de gewoonste zaak van de wereld. Een prima ontwikkeling, zeker met een heel goede en snelle verbinding.

Binnen de school zijn afspraken gemaakt over het gebruik van nieuwe media. De afspraken zijn uitgewerkt in het protocol ‘Mediawijs’.

Uitgangspunten:

- In eerste instantie is internet alleen via de proxy server van Qlict te benaderen. Via deze proxyserver is het mogelijk per gebruiker of gebruikersgroep contentfiltering toe te passen. De school bepaalt zelf of contentfiltering wordt toegepast en kan dit contentfilter via een white- en blacklist aanpassen. Alle groepen, leerkrachten en overige gebruikers mailen met webmail van onze stichting SPOOR. Wanneer er een mailbox voor de groep is aangemaakt dan beheert de groepsleerkracht deze en is verantwoordelijk voor de inkomende en uitgaande mail;
- Het meenemen van een mobiele telefoon is alleen toegestaan na toestemming van de leerkracht en is op eigen risico;
- Regelmatig communiceren over negatieve, maar vooral ook positieve invloeden van de nieuwe media.

November 2010

1. INTERNET/E-MAIL

1.1 Algemeen

Leerlingen moeten in staat zijn m.b.v. 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 kan niet. 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 van internet, maar vooral ook de voordelen van internet.

1.2 Enkele voordelen

- 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;
- E-mail kan ook door de leerlingen worden gebruikt om informatie uit te wisselen. In verband met de veiligheid hebben alle groepen één e-mailadres per groep gekregen. De groepsleerkracht is verantwoordelijk en beheert de inkomende en uitgaande mail;

- Alle personeelsleden van de .....school in dienst van het schoolbestuur (SPOOR) beschikken over een eigen e-mail adres. Met instemming van de directie wordt door de ICT-er van de school een e-mail adres toegewezen aan een andere gebruiker vanwege haar/zijn activiteiten voor de .....school.

1.3 Enkele risico's

- Niet alle plaatsen op internet zijn geschikt voor kinderogen. 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 (Hyves, Facebook, MSN) 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.
Bedenk dat:

- Het gebruik van social media 'real time' gebeurt. Een druk op de knop en jouw bericht staat direct online;
- Online informatie misschien wel eeuwig online staat. Het is niet altijd gemakkelijk om informatie naderhand te (laten) verwijderen;
- Het not-done is om eenmaal geplaatste berichten zomaar te verwijderen. Met een druk op de knop (real time) worden ook foute berichten online geplaatst.;
- Social media soms als gevolg hebben dat er een grijs gebied ontstaat tussen privé en werkgerelateerde zaken. Zorg dat er nooit een "brug" is tussen werk en privé. De interpretatie van anderen kan je behoorlijk in de problemen brengen.
- Wij kunnen op dit moment niet voorzien op welke manier er in de toekomst gebruik en misbruik wordt gemaakt van de sociale media. Deze lijst met risico's zal een dynamische lijst blijken.

1.4 Gebruikersvoorwaarden

- Leerlingen worden goed begeleid; zij worden door de leerkrachten gewezen op welke manieren zij informatie kunnen zoeken, verwerken en uitwisselen;
- Leerkrachten beschikken over voldoende internetvaardigheden;
- Leerkrachten en ouders zijn zich bewust van de risico's van internet;
- De leerkrachten volgen de verrichtingen van de leerlingen; laten tonen wat ze hebben gedaan op internet ('begeleidend confronteren'). 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. De systeembeheerder (QLICT) en de ICT- coördinator van de school zijn verantwoordelijk voor het beheer van de beveiligingssoftware en het onderhoud daarvan.
- 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);
- 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 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, of gebruikersnamen 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 Schoolafspraken

- 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. Voor inschrijvingen en wedstrijden kan ik beter een gratis (bijv. Hotmail) account aanmaken;
- Chatten mag ik niet op school;
- 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 sex, 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 met e-mail om opdrachten die ik van mijn leerkracht krijg uit te voeren.
- Deze schoolafspraken worden 2 maal per jaar met de leerlingen besproken.
- De regels die uit deze schoolafspraken voorkomen zijn bij elke werkplek te lezen.

Tips om de eigen privacy te beschermen

Thuis chatten, hyven en MSN-en:

- 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;
- Bel niet zomaar met kinderen die je van de chat kent, en spreek niet met ze af, zonder dat je ouders 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.

2. **MOBIELE TELEFOON**

2.1 Mobiel kan alles

De meeste kinderen gebruiken hun mobiele telefoon om te bellen en te sms'en, maar voor bijna driekwart is het ook een *wekker*, *horloge*, *mp3-speler* en *fototoestel*. Ook speelt meer dan de helft er *spelletjes* op. Jonge kinderen hebben bij uitzondering *internet* op hun mobiele telefoon (4%), maar van de tieners heeft al 20% internet via de mobiele telefoon
Ook binnen de .....school neemt het bezit van de mobiele telefoon toe. Veel ouders willen dat hun kind goed bereikbaar is na schooltijd.

2.2 Enkele voordelen:

- **Veiligheid:**

  Voor jonge kinderen is de mobiele telefoon vooral een veiligheidsvoorzorg**:** 90% van de 8- tot 12-jarigen heeft zijn eerste mobieltje gekregen om bereikbaar te zijn voor het thuisfront**.** Ruim de helft zegt zelfs dat ze hun mobiele telefoon alleen hebben voor in noodgevallen. Driekwart belt alleen met ouders, en dan ook nog sporadisch. Sms'en doen jonge kinderen ook niet veel.

- **Contact met vrienden (sociale netwerken):**

  In groep 8 en de overgang naar de middelbare school, wordt voortdurend contact met vrienden belangrijker. Dan hebben ze allemaal een mobiel en neemt het bellen en sms'en toe, vooral met vrienden en minder met familie. De foto's die tieners met hun mobiele telefoon maken, veranderen ook: de helft van de 13- tot 18-jarigen maakt foto's van hun familie en driekwart van hun vrienden en vriendinnen. Jongere kinderen maken juist vaker foto's van hun familie dan van vrienden.

- **Multimediale functies:**

  Bellen, sms'en, horloge, mp3-speler, fototoestel, spelletjes, internet, GPS en Google maps (navigatie), MSN'en of Hyven.

2.3 Enkele risico's

De mobiel kan tot onaangename financiële verrassingen leiden.

Van de 8- tot 12-jarigen is 10% al wel eens in de val getrapt van zo'n zogenaamd gratis ringtone of andere sms-dienst. Van de 13- tot 18-jarigen is dat al een kwart! De kosten daarvan, zo'n 9 euro per week, lopen snel in de tientallen euro's en vaak is de schade een paar honderd euro. Alle kinderen zien de reclames via tv en internet voor dit soort diensten en 50% zegt ze zelfs dagelijks te zien. Stemmen via tv-programma's als Idols, So You Think You Can Dance, en TMF Awards kost ook aardig wat, net als sms-spelletjes van sommige populaire radioshows.

- **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 lokt het met name bij sociale netwerken als Hyves, Facebook, MSN en e-mail uit tot het gebruik van grof of kwetsend taalgebruik.

- **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;

- **Zijn er afspraken gemaakt?**

  Een derde van de 8- tot 12-jarigen heeft geen afspraak met hun ouders over het bedrag waarvoor ze mogen bellen en sms'en. Voor drie op de vijf kinderen gelden geen regels over hoe vaak en hoe lang ze mogen bellen en met wie. Tweederde van de kinderen is niets verteld over telefoongedrag (wanneer zet je je telefoon uit; bijvoorbeeld op de fiets, feestje of in het theater) en welke spelletjes ze hoe lang mogen spelen. Bij driekwart van de kinderen is geen afspraak gemaakt over waar ze wel en niet foto's van mogen maken. Bij een op de vijf kinderen zijn thuis helemaal geen regels afgesproken.

2.4 Gebruikersvoorwaarden

- De mobiele telefoon; wordt ingeleverd bij de juf en is uitgeschakeld tijdens de lestijd.
- Alleen de leerkracht kan bij bijzonder omstandigheden toestemming geven de mobiele telefoon in de klas te gebruiken;
- In de ochtendpauze wordt de mobiele telefoon niet gebruikt en blijft uitgeschakeld;
- Kinderen die in de middagpauze overblijven gebruiken de mobiele telefoon niet en deze blijft ook nu uitgeschakeld;
- In noodgevallen is ieder kind tijdens schooltijd **altijd bereikbaar** onder het vaste nummer van de school (…….);
- De school is niet aansprakelijk voor het wegraken van de mobiele telefoon;

Het meenemen van de mobiele telefoon is op eigen risico.

3. OVERTREDEN GEDRAGSCODE INTERNET EN E-MAIL

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

- Wanneer er sprake is van Cyberpesten, gaat het stappenplan genoemd in bijlage 1 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 de betrokken leerling in kennisgesteld door de directie van de school. Daarbij wordt 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.
- De ICT-er/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.

4. OVERTREDEN GEDRAGSCODE MOBIELE TELEFOON

- Wanneer er sprake is van Cyberpesten, gaat het stappenplan genoemd in bijlage 1 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 kennisgesteld door de directie van de school. Daarbij wordt de aard van de overtreding vermeld en waarom de mobiele telefoon voor onbepaalde tijd is ingenomen. De betrokken ouders kunnen de mobiele telefoon na schooltijd komen ophalen.

5. 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 mobiele telefoon.
- De 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 is na te lezen op …….
- Een schriftelijk exemplaar van de gedragscode kan bij de directie worden ingezien.
- In opdracht van het schoolbestuur en de directie zijn de externe systeembeheerder, QLICT en de ICT-er van de school 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 anti-virussoftware, de fire wall, de spam-filter en de updates van de contentfiltering en beveiligingssoftware. **KPN/XS4ALL** beheert en onderhoudt de ADSL 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: SPOOR beheert en onderhoudt de mailserver. Vanaf oktober 2010 loopt het mailverkeer via webmail van SPOOR. Alle gebruikers binnen de .....school w.o. ook de groepen krijgen van SPOOR een mailadres. De eindverantwoording voor het gebruik van mobiele telefoons, internet, chatten en e-mail binnen school ligt altijd bij het schoolbestuur (SPOOR). Het schoolbestuur 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)
- www.stichtingspoor.nl