

# Veiligheid op de elektronische snelweg

## Mytylschool Ariane de Ranitz

februari 2009

### Meldingen en klachten computer/gsm-misbruik

#### Afhandeling intern

Bij het aanpakken van ongewenst gedrag op de elektronische snelweg adviseert de PPSI (landelijke werkgroep Project Preventie Seksuele Intimidatie) de volgende stappen:

1. Begeleiding van de klager door de vertrouwens-/contactpersoon.
2. Technisch/praktisch ingrijpen door de ICT-coördinator/systeembeheerder.
3. Sanctioneren misbruik door schoolleiding/bestuur/politie.
4. Lering trekken = preventiemaatregelen.

#### Contact-/vertrouwenspersoon

De contact-/vertrouwenspersoon blijft, net als bij iedere andere vorm van machtsmisbruik, verantwoordelijk voor de opvang van de lastiggevallen leerling of het lastiggevallen personeelslid.

#### Internet

Onderdeel van deze opvang is ook het geven van praktische adviezen om herhaling te voorkomen. Zo is het in ieder geval belangrijk om ongewenst internetgebruik te rapporteren aan de provider van de afzender. De provider, de verstrekker van het e-mailadres, staat genoemd na @, bijvoorbeeld: xs4all, Hetnet, Freeler, enzovoorts. Stuur daarbij ook voorbeelden van de ongewenste berichten mee, zodat de provider meteen weet waar het om gaat. De meeste providers zijn zo fatsoenlijk om direct in te grijpen.

De klager kan gebruikmaken van de mogelijkheid *block sender*, zodat dergelijke berichten niet meer vanaf het bewuste adres binnen kunnen komen. Bij Outlook staat onder 'bericht' of 'extra' de optie 'afzender blokkeren'. In het uiterste geval kan de klager een ander mailadres kiezen, dat beperkt bekend gemaakt wordt.

#### Gsm

De contact-/vertrouwenspersoon kan ook praktische tips geven om lastigvallen via 'mobieltjes' te beperken:

- Het nummer van de afzender verschijnt in principe in het venstertje van de mobiele telefoon. Berichten afkomstig van een bepaald nummer kunnen worden geblokkeerd.
- Als nummerblokkering geen optie is, kan de sms-functie worden geblokkeerd.
- In het ergste geval moet een nieuw (geheim) mobiel nummer worden aangevraagd.

De afzender kan echter onbekend blijven als het pestbericht is verzonden vanaf een mobiele telefoon zonder nummervermelding. Ook als de dader niet het eigen toestel gebruikt, maar dat van een ander, is de dader moeilijk te achterhalen. Bij een onbekende dader blijft het werk van de contact-/vertrouwenspersoon beperkt tot opvang van de klager en het geven van tips.

## **Msn**

De meeste scholen hebben chatten via de schoolcomputer verboden. Dit verbod kan niet voorkomen dat scholen toch te maken krijgen met uit de hand gelopen chats. Na schooltijd ontmoeten leerlingen elkaar in hun msn-groep. Soms druipt het venijn daarbij langs de ADSL. Als de leerlingen elkaar weer op school zien, kan de vlam in de pan slaan. De school kan het standpunt innemen dat zij niet verantwoordelijk is voor het chatgedrag van leerlingen. Maar de spanningen tussen deze leerlingen werken door in de schoolomgeving. Daarmee is het wel het probleem van de school geworden. Het middel is nieuw, de problemen zijn bekend: ruzie en pesten.

Ook bij het aanpakken van pesten via msn volgt de school het anti-pestprotocol:

- Gesprek met de gepeste leerling en zijn/haar ouder(s) (contact/vertrouwenspersoon en schoolleiding).
- Gesprek met de pesters en hun ouder(s)/confrontatie met geprinte chats (schoolleiding).
- Straf voor de pesters (schoolleiding).
- Begeleiding voor de gepeste leerling(en) gericht op grenzen stellen.
- Relatieherstel pester/gepeste.
- Relatieherstel ouder-groepsleerkracht/mentor.
- Werken aan positief klassenklimaat in de klas waar gepest is (groepsleerkracht/mentor).
- Lessen rondom bewust internetgebruik/chatten volgens de netiquette.
- Ouderavond specifiek voor de ouders in de klas waar gepest is.
- Ouderavond voor alle ouders over (pesten via) internet.
- Ouders vragen om thuis toezicht te houden.
- Schoolregels internetgebruik.

## **Contact-/vertrouwenspersoon en ict-coördinator/systeembeheerder**

Samenwerking tussen de contact-/vertrouwenspersonen en de ict'er/systeembeheerder is een belangrijke voorwaarde om overtredingen adequaat aan te kunnen pakken en te voorkomen.

Bij meldingen/klachten over internetporno is het zeker van belang dat de contact-/vertrouwenspersoon de systeembeheerder raadpleegt, om met elkaar te achterhalen of de ongewenste site bijvoorbeeld 'zomaar' kon verschijnen of dat de computergebruiker er gericht naar op zoek is gegaan.

In geval van hate-mail kunnen zij speuren naar de persoon van wie het bericht afkomstig is.

Als leerlingen/personeelsleden misbruik maken van andermans wachtwoord, kan dat een reden zijn om een nieuw persoonlijk wachtwoord te verstrekken. Zorgvuldigheid met wachtwoorden is geboden.

## **Schoolleiding/bestuur/klachtencommissie**

Een bijkomstigheid van digitaal misbruik is dat het aantoonbaar is met prints; er is bewijs. Als de digitale afzender bekend is, is er een *aangeklaagde* en kan de klager de interne/externe klachtenprocedure volgen: klachtafhandeling door de schoolleiding, het bestuur of eventueel na tussenkomst van de klachtencommissie.

Een dergelijke speurtocht heeft echter niet altijd resultaat. Het is lang niet altijd mogelijk om de afzender van een dergelijk bericht op te sporen. Het adres waar een mailbericht vandaan komt, is te vervalsen.

Afhandeling beperkt zich in zo'n geval tot emotionele ondersteuning van de klager, omdat een *aangeklaagde* tegen wie maatregelen genomen kunnen worden, ontbreekt! Wel kunnen in algemene zin voorzieningen worden getroffen om het elektronische verkeer veiliger te maken.

### **Meld- en aangifteplicht**

Op het moment dat een medewerker van de school via internet of andere digitale middelen seksueel getinte mededelingen en/of voorstellen aan minderjarige leerlingen doet, dan treedt de *Onderwijswet Bestrijding seksueel geweld en seksuele intimidatie* in werking.

#### ***Wet bestrijding van seksueel geweld en seksuele intimidatie in het onderwijs***

#### ***Meld- en aangifteplicht (1999)***

#### **Artikel 4 Verplichting tot overleg en aangifte inzake zedenmisdrijven**

1. Indien het bevoegd gezag op enigerlei wijze bekend is geworden dat een ten behoeve van zijn instelling met taken belast persoon, zich mogelijk schuldig maakt of heeft gemaakt aan een misdrijf tegen de zeden als bedoeld in titel XIV van het Wetboek van Strafrecht jegens een minderjarige leerling van de school, treedt het bevoegd gezag onverwijld in overleg met de vertrouwensinspecteur.
2. Indien uit het overleg bedoeld in het eerste lid, moet worden geconcludeerd dat er sprake is van een redelijk vermoeden dat de desbetreffende persoon zich schuldig heeft gemaakt aan een misdrijf als bedoeld in het eerste lid jegens een minderjarige leerling van de school, doet het bevoegd gezag onverwijld aangifte bij een opsporingsambtenaar als bedoeld in artikel 141 van het Wetboek van Strafvordering, en stelt het bevoegd gezag de vertrouwensinspecteur daarvan onverwijld in kennis.
3. Indien een personeelslid op enigerlei wijze bekend is geworden dat een ten behoeve van de school met taken belast persoon zich mogelijk schuldig maakt of heeft gemaakt aan een misdrijf bedoeld in het eerste lid jegens een minderjarige leerling van de school, stelt het personeelslid het bevoegd gezag daarvan onverwijld in kennis.

### **Afhandeling via politie**

Het kan zijn dat een bericht per gsm of e-mail, aanleiding geeft tot aangifte bij de politie als de inhoud in ernstige mate ontoelaatbaar is: discriminerend, racistisch, intimiderend, bedreigend, enzovoorts. Er kan aangifte gedaan worden op basis van 'stalking/belaging' of 'smaad/aantasting goede naam'.

Bij een bekende dader dient de politie aangifte op te nemen en actie te ondernemen om de zaak voor de rechter te brengen. Bij een onbekende dader dient de politie de dader op te sporen. Op de website [www.centraalmeldpunt.nl](http://www.centraalmeldpunt.nl) staan adviezen.

### **Bewijs**

Het bericht tonen (op het gsm-scherm/met een uitdraai) aan politie of de officier van justitie maakt meteen duidelijk om welk gedrag het gaat. Ook kan dit dienen als bewijsmateriaal. Maar zelfs met bewijs is opsporing niet makkelijk. Onderzoek kost tijd en moeite en soms de kosten van een advocaat. De recherche is namelijk afhankelijk van de medewerking van de provider om het ip-adres te achterhalen. De provider komt pas in actie na een rechtshulpverzoek van een advocaat. Als er gebruik is gemaakt van een internetcafé of een proxyserver, is de dader bijna niet te achterhalen.

Als de politie na onderzoek een verzoek indient bij de officier van justitie om de zaak in behandeling te nemen, dan is het de vraag of justitie hieraan gevolg geeft, omdat dergelijke zaken moeilijk te bewijzen zijn. En als justitie vervolgt, dan is er

veelal nog een lange weg te gaan. Een zaak uit 2002, waarbij een leerling een medeleerling op een sekssite aanbood, loopt in 2006 nog steeds in hoger beroep. Voorkomen is beter dan genezen!

### **Gsm-/cyber-stalking**

Leerlingen en personeelsleden kunnen zich belaagd (gestalkt) voelen, doordat zij herhaaldelijk worden lastiggevallen. Sinds 2000 is een anti-stalkingswet van kracht: artikel 285B van het Wetboek van Strafrecht. Daarmee is de mogelijkheid geopend om de politie in te schakelen.

### **Smaad**

Leerlingen en personeelsleden die met naam- en adresgegevens zijn aangeboden op seks-sites, kunnen aangifte doen op basis van smaad:

#### **Artikel 261/Sr, Boek 2, Titel 16**

1. Hij die opzettelijk iemands eer of goede naam aanrandt, door telastlegging van een bepaald feit, met het kennelijke doel om daaraan ruchtbaarheid te geven, wordt, als schuldig aan smaad gestraft met gevangenisstraf van ten hoogste zes maanden of geldboete van de derde categorie.
2. Indien dit geschiedt door middel van geschriften of afbeeldingen, verspreid, openlijk tentoongesteld of aangeslagen, of door geschriften waarvan de inhoud openlijk ten gehore wordt gebracht, wordt de dader, als schuldig aan smaadschrift, gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de derde categorie.

### **Foto's van leerlingen**

Lang niet alle ouders stellen het op prijs als een foto van hun kind op de school-website worden gezet. Bijvoorbeeld omdat zij op de vlucht zijn voor een mishandelende partner of omdat zij misbruik vrezen door pedofielen. Om manipulatie van digitale foto's te bemoeilijken, besluiten steeds meer scholen om geen foto's meer van individuele kinderen op de school-website te plaatsen, maar uitsluitend van groepjes. Namen en andere persoonlijke gegevens worden niet gepubliceerd bij de foto om zo de privacy te beschermen.

### **Wet Bescherming persoonsgegevens (WBP)**

Vooraf dient de school toestemming te vragen aan ouders voor het fotograferen en het publiceren van foto's van hun kinderen. Dat is conform de Wet Bescherming persoonsgegevens die per 1 september 2001 in werking is getreden. In het kort komt de wet er op neer dat bedrijven en instellingen toestemming moeten vragen voor het gebruik van persoonsgegevens als de openbaarmaking van die gegevens herleidbaar is naar individuele persoonsgegevens.

### **Fotorecht**

Het fotorecht bepaalt dat opnames niet zonder toestemming van degene die gefotografeerd of gefilmd is, verspreid mogen worden. Leerlingen die anderen ongevraagd te kijk zetten op gsm's, internet of in print op schoolprikborden, zijn conform dit fotorecht strafbaar. Als het fotorecht geschonden is, kan de klager op basis hiervan aangifte doen.

### **Preventiemaatregelen**

Ingrijpen bij klachten wordt makkelijker als de school regels kent voor digitaal verkeer. Naast omgangsvormen, tafelmanieren en verkeersregels is het belangrijk

dat leerlingen en personeel ook de elektronische snelweg gebruiken volgens een netetiquette/nettiquette. De school formuleert daarvoor duidelijke regels en treedt op als leerlingen en personeel zich daar niet aan houden. De regels worden besproken en zijn duidelijk zichtbaar (bijvoorbeeld op het startscherm van de computer).

Hoe duidelijker de regels, hoe makkelijker een overtreding aan te tonen en te sanctioneren is. Bij sanctioneren volgt de school de gangbare procedures inzake schorsing en verwijdering van leerlingen en het Rechtspositiebesluit onderwijs-personeel. Bij minder zware vergrijpen kunnen leerlingen gestraft worden door b.v. hun gsm tijdelijk in te nemen of hen de toegang tot het schoolnetwerk te ontzeggen.

### **Personeel**

De vakbond FNV heeft een voorbeeldprotocol voor internetgebruik opgesteld, waarin staat:

#### **Protocol computergebruik personeel**

##### Artikel 2, lid 2

Het recht van de werknemer om persoonlijke e-mailberichten te ontvangen en te versturen is gebonden aan de volgende voorwaarden:

- de mail zal een disclaimer bevatten;
- het is niet toegestaan dreigende, seksueel intimiderende, dan wel racistische berichten te versturen.

##### Artikel 3

1. Werknemers zijn gerechtigd het internetsysteem voor niet-zakelijk verkeer te gebruiken, mits dit niet storend is voor hun dagelijkse werkzaamheden.
2. Het is niet toegestaan bewust sites te bezoeken die pornografisch materiaal bevatten, dan wel racistische sites.

De LKC (Landelijke Klachtencommissie) formuleert als aanbevelingen, ook voor e-mailcorrespondentie: "Dat een docent zich in de omgang met andere bij de school betrokkenen steeds bewust dient te blijven van het professionele kader" en "Dat een docent met zijn handelen een onderwijskundig doel dient".

De vertrouwensinspecteurs formuleren als uitgangspunten voor (online) contact tussen personeel en leerlingen: 'Functioneel en schoolgerelateerd'. Dus:

- Wel informatie toesturen langs de elektronische snelweg; opdrachten/werkstukken digitaal laten inleveren en becommentariëren, maar niet chatten op msn.
- Wel een afspraak maken voor een mentorgesprek, maar geen e-mentoring en al helemaal niet met leerlingen achter de webcam.
- Wel een vrij eerste uur doorbellen, geen persoonlijke gesprekken met een leerling.

Het is immers niet vanzelfsprekend dat personeel buiten schooltijd individueel contact heeft met leerlingen? Duidelijke regels bieden een kader om bij overtreding van een gebod in te grijpen.

### **Gouden regels voor leerlingen**

- Toon respect voor anderen.
- Stuur geen berichten die je zelf niet zou willen ontvangen.
- Stuur geen anonieme berichten.
- Stuur geen gemene of vervelende berichten, dus niet discrimineren, pesten of (seksueel) intimideren.
- Surf niet naar pornosites, sekssites, racistische sites, treiter-/afzeiksites, enzovoorts.
- Verspreid geen opnames van medeleerlingen en/of docenten via b.v. je gsm of e-mail.
- Vertel je wachtwoord aan niemand.
- Geef geen persoonlijke informatie (je naam, adres, telefoonnummer, naam van de school, rekeningnummer, enz.) door.
- Meld het bij de leerkracht/systeembeheerder als je vervelende berichten krijgt.

### **Praktisch**

#### **Computeropstelling**

De plaats waar computers in de school staan, kan effect hebben op het gebruik of misbruik van internet. Zet de computers bij voorkeur in een gemeenschappelijke ruimte, bijvoorbeeld in een klas waar steeds leerlingen en een personeelslid aanwezig zijn of in de gang waar regelmatig mensen passeren. Zo ontstaat een zekere mate van sociale controle.

#### **E-mailadres van de school**

Met het oog op de controleerbaarheid is het verstandig om als uitgangspunt voor e-mailcorrespondentie te nemen, dat leden van de schoolgemeenschap gebruik maken van het e-mailadres van de school en niet van hun persoonlijke e-mailadres. Op sommige scholen moet, met dit zelfde doel, eerst ingelogd worden op de schoolsite.

#### **Systeembeheer**

De systeembeheerder/ict-leerkracht heeft naast de zorg voor de hard- en de software ook een verantwoordelijkheid ten aanzien van het veilig gebruik van de internetvoorziening. Daarbij gaat het om de al genoemde fysieke opstelling, maar ook om het uitgeven van inlognamen aan leerlingen. Het is niet verstandig om makkelijk herleidbare inlognamen toe te kennen, zoals een letter van de voornaam en achternaam en het geboortejaar. Kinderen kunnen dan namelijk ook onder elkaars inlognaam gaan surfen.

Daarnaast moeten leerlingen gewaarschuwd worden om hun inlognaam niet aan iedereen te vertellen. Leerlingen moeten leren hoe ze hun privacy kunnen waarborgen. Systeembeheerders kunnen meekijken en/of via de optie 'geschiedenis' zien waar gebruikers van een computer geweest zijn en van welke internetdiensten zij op school gebruikmaken. Het is belangrijk dat de schoolgemeenschap weet dat de systeembeheerders waken over het internetgebruik en ingrijpen bij overtredingen.

#### **Camergebruik en mp3-opnamen op school**

Steeds meer mobiele telefoons zijn uitgerust met een camerafunctie. Onaangename incidenten, met als uitwas 'happy slapping', hebben ertoe geleid dat veel scholen het gebruik van de mobiele telefoon én de camerafunctie binnen school en op het schoolterrein verbieden.

Regels bieden een kader om bij overtreding van dit verbod in te grijpen:

“Geluids- en beeldopnamen mogen op de terreinen van de school alleen met instemming van de betrokkene(n) worden gemaakt. Beeld- en geluidsmateriaal dat onder schooltijd of tijdens schoolactiviteiten is opgenomen, mag niet worden vertoond aan derden, tenzij hiervoor uitdrukkelijk toestemming is verleend door de schoolleiding. Overtreding hiervan kan tot verwijdering van school leiden”.

### **Scholen ‘scholen’ op internetgebruik**

Scholen gebruiken internet voor opbouwende educatieve doelen. Zoals hierboven beschreven moeten scholen de verantwoordelijkheid nemen voor correct gebruik van het wereldwijde web door leerlingen en personeel. Daarnaast blijkt het medium minder leuke en soms zelfs gevaarlijke kanten te hebben: pornosites, loverboys, pedoseksuelen, enzovoorts.

Ook hierin kan de school een educatieve rol vervullen met tips als:

- Wees voorzichtig online.
- Geef nooit persoonlijke informatie door zoals je echte naam, adres, (mobiele) telefoonnummer, je bankpas, maar ook foto’s van jezelf of je familie laat je niet zomaar overal slingeren. Dus ook niet op internet, want je weet nooit wat anderen daarmee doen. Dat geldt ook voor de naam van je school.
- Wees zuinig met het geven van je e-mailadres.
- Pas op met de webcam, beelden kunnen opgeslagen en verspreid worden.
- Maak geen afspraak met internetcontacten.
- Internetten lijkt privé, maar wat je op het world wide web zet, blijft rondzwerven en kan je je leven lang achtervolgen!

### **Meer informatie:**

[www.besafeonline.org](http://www.besafeonline.org)  
[www.pestenislaf.nl](http://www.pestenislaf.nl)  
[www.internetsoa.nl](http://www.internetsoa.nl)  
[www.pestweb.nl](http://www.pestweb.nl)  
[www.kinderconsument.nl](http://www.kinderconsument.nl)  
[www.schoolenveiligheid/tools/internetonveiligheid](http://www.schoolenveiligheid/tools/internetonveiligheid)  
[www.mijnleerlingonline.nl](http://www.mijnleerlingonline.nl)  
[www.surfopsafe.nl](http://www.surfopsafe.nl)  
[www.msn.nl/veiligonline/leraren](http://www.msn.nl/veiligonline/leraren)  
[www.surfsafe.nl](http://www.surfsafe.nl)