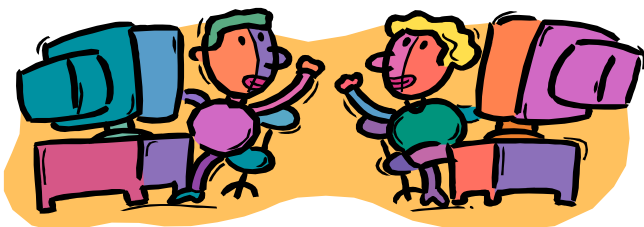


Gedragcode en internetprotocol

De computer is momenteel een informatiemedium dat niet meer is weg te denken uit onze samenleving. Iedereen heeft er mee te maken, of je dat nou wil of niet. Dagelijks krijgt iedereen te maken met apparatuur waarin computerchips zijn gebouwd. Dat varieert van het aanzetten van radio of t.v. tot autogebruik, terwijl via de



computer heel wat informatieverkeer wordt verwerkt, ontvangen en verzonden. Hierbij zijn e-mail en internet inmiddels gangbare begrippen geworden.

Net als in de “gewone” samenleving is er in de digitale wereld ook sprake van voor- en nadelen. Helaas zijn er figuren die van de digitale media misbruik trachten te maken. Wie kent niet de schadelijke computervirussen, ongewenste reclames (“spam”) en ongewenste programma’s (“spyware”, “pop-ups”) die ongevraagd – en vaak ongezien – met het digitale verkeer worden meegestuurd.

Het is van groot belang om je hiertegen te beschermen (bv. met programma’s als “firewall”), doch deze bescherming is helaas nooit optimaal. Voortdurend ontdekken kwaadwilligen wel “computerlekken” om zich ongewenst toegang te verschaffen. Het is voor elke computergebruiker van groot belang zich hiervan bewust te zijn en in zijn/haar gedrag hier rekening mee te houden, zodat je jezelf zoveel mogelijk kunt beschermen tegen de meest uiteenlopende vervelende gevolgen.

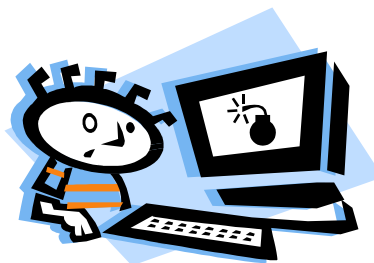
Op school geldt daarvoor een “gedragcode” en een “internetprotocol”.

Op school gelden voor leerkrachten en leerlingen de volgende gebruikersafspraken:

- Er worden geen sites bezocht met aanstootge-

vende informatie of die door de schoolleiding als ongepast worden aangemerkt.

- Er worden geen kettingbrieven of berichten met buitensporig grote informatie verzonden.
- Tijd besteden aan zaken, of e-mailberichten uitlokken die niets met onderwijs of school te maken hebben is niet toegestaan.
- Onwettige activiteiten, gokken, ontoelaatbare opmerkingen/voorstellen of materialen zijn uit den boze.
- Er wordt geen software of computerbestanden gedownload zonder toestemming of zonder virusbescherming.
- De normale werking van de computer of het computernetwerk mag niet opzettelijk worden verstoord.
- Vertrouwelijke informatie mag niet worden gepubliceerd.
- Computeraccounts, post of bestanden van anderen mogen niet zonder uitdrukkelijke toestemming worden geopend of gebruikt.



Voor de kinderen gelden de volgende 7 “gouden regels” bij het internetten: het “internetprotocol”

1. Ik mag alleen mijn voornaam gebruiken; ik geef anderen geen persoonlijke gegevens zoals mijn adres, telefoonnummer, e-mailadres, het adres van mijn ouders of van bekenden. Bij msn gebruik ik altijd een verzonden “nickname”.
2. Ik ga meteen naar mijn leerkracht of mijn ouders als ik op internet vervelende informatie tegenkom.
3. Ik zal nooit toestemming geven aan iemand die ik op internet ben tegen gekomen, in het echt te ontmoeten.

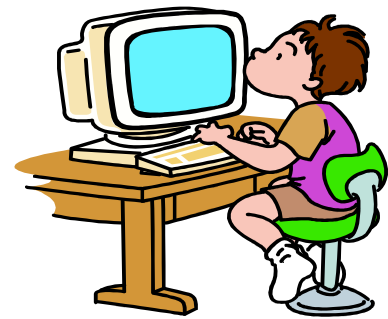
4. Ik zal “internet-personen” geen foto’s van mezelf toesturen, behalve als mijn ouders of leerkracht daar toestemming voor hebben gegeven.
5. Ik ga niet reageren op gemene, valse of vervelende berichten. Dat sommige mensen zich niet weten te gedragen is immers niet mijn schuld. Als het hele gemene ding is waar schuw ik direct de leerkracht en mijn ouders. Die kunnen dan beslissen of ze contact opnemen met de politie.
6. Als ik aan het e-mailen (of chatten, msn-men) ben, zal ik me netjes gedragen. Mijn taalgebruik is immers een goede reclame voor mezelf en voor onze school.
Chatten onder schooltijd mag alleen als de leerkracht daar toestemming voor heeft gegeven.
7. Als ik een e-mailbericht ontvang van een persoon die ik niet ken, meld ik dit meteen aan mijn ouders of leerkracht.

Consequenties

De school (directie, team) draagt er zorg voor dat iedereen die bij de school betrokken is op de hoogte wordt gesteld van de gebruikersafspraken en het internetprotocol. Bij (ernstig, doelbewust) misbruik van wil de directie van de school enkele maatregelen nemen.

In alle gevallen zal er een gesprek plaatsvinden met de betreffende leerling(en) en worden de ouders/verzorgers op de hoogte gebracht. Bij misbruik door een leerkracht of een andere bij de school betrokken volwassene wordt de directie om advies gevraagd. Er kan worden overgegaan tot een berisping door de leerkracht (als het een leerling betreft) of de directie, terwijl bij herhaling kan worden besloten tot opheffing van het e-mailadres of verwijdering uit het gebruikersbestand. Hiermee wordt de betrokkene toegang tot het internet of computernetwerk ontzegd.

Deze maatregel kan zowel een tijdelijk als vast karakter hebben, te besluiten door de directie van de school.



Gezond

achter de computer

Om gezondheidsrisico’s te voorkomen zijn er enkele zaken waarop gelet moet worden bij het werken achter de computer.

Van belang is om een goede zithouding aan te nemen. Hierbij is het zaak te letten op voldoende steun voor voeten en een rechte rug, terwijl aanbevolen wordt het scherm op ooghoogte (of zelfs lager!) op te stellen. Bij veel computertafels is dat niet het geval en staat de monitor zelfs op een verhoging. Dat kan leiden tot ernstige nekklachten.

Ook een gezonde duur van werken met de p.c. is aan een maximumtijd gebonden. In het bedrijfsleven gelden arbo-regels, waarin gesteld wordt dat medewerkers maximaal anderhalf uur aan één stuk achter het scherm mogen zitten.

Afwisseling met activiteiten waarbij andere lichaamsbewegingen worden aangesproken zijn daarna een “must”.

Voor kinderen dient deze tijd uiteraard te worden aangepast: hoe lager de leeftijd, hoe lager de computertijd en hoe hoger de afwisseling in activiteit dient te zijn.

Website

Informatie opvragen via internet is algemeen gangbaar geworden en vrijwel alle instanties verlenen deze via een eigen website.

Informatie over ons schoolbestuur Innovo is voor iedereen eenvoudig op te vragen via de site www.innovo.nl vanaf welke plaats u kunt doorlinken naar de informatiepagina’s van de diverse scholen van het bestuur.

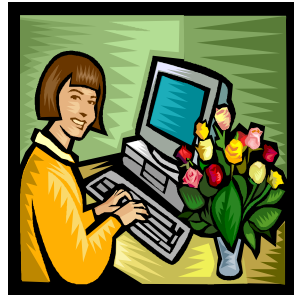
Verder heeft de school de beschikking over een eigen website. Op onze site zijn ook foto’s ter illustratie geplaatst, die gedurende een schooljaar kunnen worden gewijzigd op basis van actualiteit. Een stukje tekst over een school- of werkgroepactiviteit zal immers meer aanspreken als er (informatief) beeldmateriaal aan is toegevoegd.



In verband met veiligheid en de bescherming van privacygegevens zullen we daar echter voorzichtig mee omgaan. Zo zullen er bv. geen foto's en naam- en adresgegevens van personen aan elkaar gekoppeld worden.

Goede informatie hierover is te vinden op de site: www.mijnkindonline.nl

We kunnen ons voorstellen dat zowel ouders, kinderen en leerkrachten bezwaar kunnen hebben tegen het wereldwijd bekend maken van hun gegevens bij de schoolinformatie.



Behalve het plaatsen van (groeps-)foto's denken we daarbij ook aan het verspreiden van adresgegevens, telefoonnummers e.d. Daarom zal uit voorzorg de website, inclusief tussentijdse wijzigingen, voortdurend kritisch bekeken worden

Vragen

Ook indien u t.a.v. andere schoolse computerzaken vragen of opmerkingen heeft kunnen deze gericht worden aan de coördinator Informatie en Communicatie Technologie van onze school. Indien bv. een ouder bezwaren heeft tegen het uitreiken van een webadres aan het kind, dient met hem contact op te worden opgenomen. Het internetadres van het kind kan dan ongedaan worden gemaakt.

Om enige ervaring op te doen zal op de schoolcomputers met de kinderen "geoefend" worden. In elke groep, óók in de onderbouw, staan computerlessen in het weekrooster opgenomen.

PESTEN VIA INTERNET

Hoe begeleid je als ouder je kind op Internet? Hoe zorg je dat kinderen zorgeloos, veilig op het net kunnen vertoeven? Door betrokken te zijn bij wat ze doen. Geen enkele ouder stuurt zijn kinderen zomaar de straat op, de grote stad in. Je vertelt ze wat ze daar kunnen verwachten, wat leuk is en wat niet, wat wel mag en wat niet. En in het begin blijf je er een beetje bij. Hetzelfde zou eigenlijk voor Internet moeten gelden. Maar dan moet je natuurlijk wel weten waar het over gaat.

De website 'Mijn kind online' (www.mijnkindonline.nl) ondersteunt ouders bij veilig Internet-gebruik door hun kinderen.



Hulp aan het gepeste kind

1. Negeer pest-mails. Internet-pesters kunnen gemakkelijk anoniem blijven. Daarom is het vaak niet mogelijk om een dader te achterhalen en zit er niets anders op dan het effect te minimaliseren. Dat kan het beste door niet te reageren op haatmailtjes of andere ongewenste e-mail. Als de dader geen respons krijgt, gaat de lol er snel af.
2. Blokkeer afzender mail of blokkeer MSN'er. Het is zo simpel, zonder dat degene die je blokkeert het door heeft.
3. Als er iets vervelend gebeurt in de chat, ga dan weg.
Log eventueel opnieuw in met een andere bijnaam (nickname).
4. Vat scheldpartijen of beledigingen niet persoonlijk op, zeker als het komt van mensen die je niet kent. Vaak zegt men vervelende dingen uit verveling.

5. Als het pesten aanhoudt en je je ongemakkelijk of bedreigd voelt, ga dan naar je ouders of heb het erover met iemand die je vertrouwt.
Erover praten: heel belangrijk. Heb het er met iemand over die veel van computers en internet weet en die niet meteen iedereen vertelt dat je gepest wordt.
6. Als je gepest wordt via internet, bewaar het. Bewijs!
7. Voel je niet schuldig als er iets vervelends gebeurt. Het is niet jouw schuld en je hebt het niet zelf uitgelokt.

Tips voor ouders van via internet gepeste kinderen

Hoe zorg je dat kinderen zorgeloos, veilig op het net kunnen vertoeven? Door betrokken te zijn bij wat ze doen.

Geen enkele ouder stuurt zijn kinderen zomaar de straat op, de grote stad in. Je vertelt ze wat ze daar kunnen verwachten, wat leuk is en wat niet, wat wel mag en wat niet. En in het begin blijf je er een beetje bij. Hetzelfde zou eigenlijk voor Internet moeten gelden. Maar dan moet je natuurlijk wel weten waar het over gaat. De beste tips krijgt u van collega-ouders die, net als u, kunnen putten uit de praktijk.

1. Reageer niet op pest-mails. Negeren ontmoedigt de pesters.
2. Vertel ze dat ze pest-mails bewaren als bewijs.
3. Praat met de school over het antipestbeleid.
Als het pesten in de klas wordt aangekaart, bestaat het gevaar dat het slachtoffer opnieuw door de pester(s) te grazen wordt genomen. Dat gevaar is echter kleiner wanneer de school een goed anti-pest-beleid hanteert. Bespreek dit met een leerkracht of met de directie.
4. Praat erover met andere ouders, bijvoorbeeld via het discussieforum van Ouders Online (www.ouders.nl).
5. Maak een melding bij de wijkagent of, als het echt ernstig is, doe aangifte. Bij een melding onderneemt de politie geen actie. Er wordt geen proces-verbaal opgemaakt en men gaat niet op zoek naar de dader. Er gebeurt dus verder niets, maar het voordeel is wel dat de

politie op de hoogte is. Een melding kan van belang zijn voor eventuele vervolgmeldingen of andere (latere) aangiftes. Tijdens de melding kunt u tegelijkertijd informeren wat de gevolgen zijn van het doen van aangifte.

6. Neem uw kind serieus, maar leer hem of haar ook te relativiseren. Een kind denkt al snel dat het zijn eigen schuld is dat hij gepest wordt. Probeer dat schuldgevoel te voorkomen en neem alles waarmee uw kind zich tot u wendt serieus. Het komt niet gauw in een kind op om te denken dat iemand 'voor de lol' een hatemail stuurt en dat het eigenlijk helemaal niet speciaal voor jou bedoeld is, terwijl het vaak wel zo gaat. Je hebt het dus niet in de hand dat iemand zulke mail naar je stuurt, maar je kunt wel zelf bepalen in hoeverre je jezelf er door laat beïnvloeden. Wimpel het probleem niet weg, maar probeer het wel wat te relativiseren.



Algemene tips voor ouders

1. Zet de pc op een centrale plek in de woning.
2. Leer uw kind wat netiquette is. Onder netiquette verstaan we: de gedragsregels op het Internet. Leer uw kind altijd vriendelijk, eerlijk en beleefd te blijven, en niet (terug) te gaan schelden als iemand vervelend doet. Online gelden dezelfde omgangsvormen als offline. En wat anderen kunnen, kan uw eigen kind natuurlijk ook.. Denk niet dat uw eigen kinderen altijd het lieverdje zijn. Ook zij kunnen andere kinderen uitdagen, pesten of lastigvallen. Ze kunnen zich anders voordoen dan ze zijn. Zorg dat ze geen lompe berichten of bedreigingen posten. Wie zich bij het chatten en mailen aan dit soort fatsoensregels houdt, zal zelf ook minder snel in de problemen komen.

3. Hang de "vuistregels" (deze zijn te downloaden van de website *Mijn Kind Online .nl*) naast de computer.
4. Weet waar u het over hebt. Zorg dat u zelf genoeg weet van Internet, om te begrijpen waar uw kind mee bezig is. Maak uzelf vertrouwd met de belangrijkste mogelijkheden. Ga chatten, MSN-en, surfen en zoeken, downloaden en mp3'tjes delen. Alleen op die manier kunt u uw kind echt webwijs maken.
5. Praat over internet. Praat regelmatig met uw kinderen en hun vrienden en vriendinnen over wat ze doen en meemaken op Internet, en hoe ze dat vinden. Vertel ook over uw eigen ervaringen. Op die manier laat u weten dat u ontvankelijk bent voor hun ervaringen en zullen ze eerder naar u toekomen als dat nodig is.
6. Installeer een goede virusscanner. Kinderen sturen elkaar soms virussen toe. Als 'geintje'.

Tips voor alle kinderen

1. Tel tot tien als je ergens over geïrriteerd bent op internet/msn, zeg geen dingen waar je later spijt van krijgt
2. Een geintje hoeft niet altijd als een geintje over te komen. Stuur je iemand een virus via MSN bijvoorbeeld, dan lijkt dat misschien heel amusant. Maar een computer kan zo vast lopen dat er veel geld moet worden besteed om de computer te repareren.
3. Zet geen informatie over anderen op je eigen homepage, ook niet voor de grap.
4. Bewaar je wachtwoord voor je mail en MSN zorgvuldig en geef ook niet te snel je mailadres weg. Inbreken op het account van een ander is een strafbaar feit. Je geeft je adres en telefoonnummer ook niet zomaar aan iemand, dus ook niet op internet.
5. Blijf aardig en vriendelijk, wees niet lomp.

Bron: *Mijn kind online (KPN-site)*



Internet en school: achtergrondinformatie

Privacy van de leerlingen

Veel scholen hebben een eigen website. Zo'n site heeft verschillende functies en bij alle functies moet nagedacht worden over de privacy van de leerlingen.

Functies van een schoolsite

□ **marketing** - school-websites worden onder andere gebruikt voor het presenteren van de school aan buitenstaanders. Ouders die nog geen kind op deze school hebben, kunnen zich dan oriënteren en vaak staat de complete schoolgids online. Ook bevat zo'n site meestal de contactgegevens van de directie of de administratie, en soms kom je zelfs persoonsgegevens van de leerkrachten tegen.

Om de sfeer te laten proeven staan er vaak ook foto's op de website. Zowel van het schoolgebouw (van binnen en van buiten), als van de omgeving. Maar vaak ook van leerkrachten en van leerlingen. Met name dat laatste kan een inbreuk op de persoonlijke privacy vormen. Leerkrachten en leerlingen hebben er immers niet om gevraagd om zich te laten portretteren voor de hele wereld, laat staan voor marketingdoeleinden.

□ **schoolnieuws** - een tweede functie van de school-website is om ouders van bestaande leerlingen te informeren over de dagelijkse gang van zaken. Soms staan de nieuwsbrieven van de school online en kun je notulen van vergaderingen terugvinden. Ook kun je vaak schoolafspraken nalezen en het jaarprogramma inzien. In het verlengde hiervan is er soms een afgeschermd gedeelte voor het personeel (ten behoeve van hun onderlinge communicatie), maar het komt ook voor dat buitenstaanders daar ook gewoon kunnen meelesen.

□ **speeltuin** - tenslotte kan de school-website bedoeld zijn voor de leerlingen zelf. Als het een beetje meezit kunnen zij hun eigen materiaal op de website publiceren, al of niet onder leiding van de leerkrachten.

Nadenken over Privacy

Het is verbazingwekkend hoe vaak scholen zomaar van alles op hun website publiceren. Alsof er helemaal niet nagedacht wordt over de gevolgen wanneer je iets openbaar maakt.

In het enthousiasme voor het maken van een aantrekkelijke website komt het vaak voor dat er foto's van leerlingen worden gepubliceerd, met hun namen en leeftijden erbij en soms ook nog met e-mail adressen. Lang niet altijd gebeurt dat met medeweten van de leerlingen, laat staan dat zij (of hun ouders) daarvoor toestemming hebben gegeven.

Ouders die hiertegen protesteren, stuiten regelmatig op onbegrip. Vaak vindt men de bezwaren van de ouders overdreven, maar dat zijn ze zeker niet. Ouders hebben de plicht om hun kinderen te beschermen en scholen hebben de taak om ouders daarin te ondersteunen.

Kortom: let erop dat de school van uw kind de privacy van de leerlingen waarborgt. Het is niet meer dan normaal dat ouders hierover vragen stellen aan de school, of een gesprek aangaan over het beleid.

Privacy-richtlijnen

De onderstaande richtlijnen zouden bij het normale ICT-beleid van de school moeten horen (bron: Brochure 'Klikvast – ook op de informatiesnelweg' van het Vlaams departement onderwijs).

1. Zorg dat er geen koppeling bestaat tussen namen en foto's. Zo reduceer je de kans dat mensen buiten de school belang gaan stellen in het kind. Dus:

- als de naam van een leerling genoemd wordt, gebruik dan geen foto;
- als je een foto gebruikt, laat dan de naam van de leerling weg.

2. Vraag de toestemming van de leerlingen én van de ouders wanneer u foto's van kinderen gebruikt op de school-website. Zo komt niemand voor verrassingen te staan.

3. Gebruik niet alleen portretten om de website te verlevendigen. Ook een panorama, een detailopname uit de klas, of ingescand lesmateriaal kan de moeite waard zijn.

4. Vraag aan de leerkrachten of zij willen dat hun gegevens beschikbaar zijn op het Internet.

Niet alle leerkrachten zullen het fijn vinden als hun privé-gegevens (portret, naam, adres, telefoonnummer) op de website staan.

Tot slot

Voor de leerlingen is het belangrijk dat ze weten bij wie ze terecht kunnen met vragen en problemen over Internetgebruik op school. Bij wie kunnen ze nare ervaringen melden? Bij wie kunnen ze discriminerende, extreem gewelddadige of andere grensoverschrijdende website melden?

- Praten is veiliger dan zwijgen

Pubers zijn snel geneigd te zwijgen, omdat hun leerkrachten zo weinig weten van Internet. Dat is jammer, want praten kan de veiligheid aanzienlijk verhogen.

De kans is groot dat kinderen op school liever zwijgen over nare ervaringen dan dat ze een leerkracht in vertrouwen nemen. Waarom?

Omdat deze kinderen wel doorhebben dat leerkrachten vaak zelf niet voldoende van het Internet weten om hen te kunnen helpen. Erger nog, dat bange leerkrachten bij de minste dreiging van onveiligheid reageren met het instellen van verboden.

Een kind dat zijn behoefte aan hulp of gewoon een gesprek beloond ziet met een toename van beperkingen op de eigen vrijheid, zal geneigd zijn te zwijgen. Het is duidelijk dat dat onwenselijk is.

- Thuis

Ouders hebben maar weinig invloed op het tempo waarin de school de nieuwe ontwikkelingen bijbeent. Er zit dus niets anders op dan ervoor te zorgen dat uw kinderen in ieder geval thuis terecht kunnen.

Docenten, vaders, moeders, etc., die zich *niet* laten leiden door angst maar door kennis, daar kan een kind op bouwen. En de veiligheid die dat biedt voor een kind, daar kan geen Internetfilter tegenop.