



basisschool Heiveld
kleuterschool en lagere school

ICT: informatie voor de ouders



Heiveldstraat 127A 904 GENT

++32 9 228 87 65 ++32 9 238 29 13

BSHEVELD.SJC-GENT.BE VBS.HEVELD@SJC-GENT.BE



10 maart 2010

uw kind: computer en gsm, thuis en op school

1. info beleid voor ouders:

Onze school ontwikkelt een visie over Informatie en Communicatie Technologie als leermiddel en -doel. ICT is veel meer dan enkel 'de computer in de klas': het omvat alle moderne middelen om te communiceren en informatie te verwerken.

De ICT-coördinator ondersteunt diverse activiteiten op school om de verplichte eindtermen ICT op het einde van de basisschool te bereiken. De klassentitularis integreert ICT in de organisatie van zijn klassenpraktijk. A.d.h.v. zorgvuldig gekozen hard- en software krijgen kinderen kansen om te 'groeien' en zich te ontwikkelen. Voor concrete opdrachten kunnen ze hierbij het ICT-materiaal van onze school gebruiken.

De kinderen leren in onze basisschool zelfstandig en veilig met ICT-media om te gaan. Dit gebeurt stapsgewijs: bij de jongsten worden de programma's duidelijk afgebakend door de leerkracht. De oudsten krijgen een grotere keuzevrijheid en verantwoordelijkheid om een educatieve opdracht te verwerken. In de vierde klas krijgen alle leerlingen een basiscursus typen aangeboden

Met een ICT-protocol (lijst van regels) voor leerlingen beogen we een vlot en veilig gebruik van ons computerpark. Wanneer kinderen op de computer werken, is er niet altijd een leerkracht in de nabije buurt. Een firewall biedt dan bescherming tegen ongewenste sites.

2. schoolbrochure: privacy

Wij respecteren de privacy van onze leerlingen en hun familie. Indien u uw (e-mail)adres, telefoonnummer, foto van uw kind niet wenst te delen met anderen, laat u dit best weten via de zorgcoördinator.

3. veilig online

-voor ouders met jonge kinderen: installeer bijv. de browser: 'MyBee'

-voor ouders van tieners: www.veiligonline.be – werk met een updatet antivirusprogramma* – maak voor uw kind een lijst met de betere favoriete zoeksites – stel duidelijke regels i.v.m. profiel en delen van gegevens op o.m. sociale netwerksites.

*freeware: AVG, Avast, Avir, Microsoft Security Essentials

schoolbestuur
scholengemeenschap
SINTJAN-VISITATIE.BE

vzw basisscholen Sint-Jan & Visitatie – Antwerpsesteenweg 988 – 9040 Sint-Amandsberg

filip.bogaert@sintjan-visitatie.be

++32 479 69 55 80

interessante zoeksites voor jongeren

- www.jeugdbieb.nl
- www.wikipedia.be – www.wikikids.be
- www.webwijzer.bibliotheek.be
- www.netwijs.nl
- <http://users.skynet.be/zoekheteensop/>
- www.meestersipke.nl
- www.kids.kennisnet.nl
- www.webkwestie.nl
- www.look4.be
- www.kidzz.be
- www.ICT-platform.be
- <http://www.schooltv.nl/beeldbank/>
- www.google.be (gebruik Google liefst enkel om afbeeldingen te zoeken)

veelgestelde vragen: antwoorden op 'veiligonline.be'

Installatie (9)

[Kan men inbreken op mijn harde schijf?](#)

"Pas op of ik hack je computer" of "ik blokkeer je MSN" is een dreigement dat vaak door cyberpesters gebruikt wordt. We gaan niet ontkennen dat hacken bestaat, maar je moet al behoorlijk wat kaas gegeten hebben van informatica om hier echt goed in te zijn. Er zijn dus maar weinig mensen die dit effectief kunnen. Zo'n dreigementen zijn dan ook vaak niets meer dan bluf.

Anderzijds denken mensen soms dat er iemand ingebroken heeft in hun computer omdat deze plotseling vreemde dingen doet. Vaak ligt er eerder een virus aan de basis van deze problemen.

[Hoe kan men weten op welke websites de kinderen zaten?](#)

Je doet er goed aan om regelmatig samen met je kinderen te surfen en hen te vragen welke websites ze bezoeken.

Je kan ook samen eens hun Tijdelijke Internet Bestanden of Temporary Internet Files bekijken (in je Explorer ga je naar Tools -> internet options -> general -> browsing history -> view files of Extra -> internet opties -> algemeen -> browsegeschiedenis -> instellingen -> bestanden weergeven). Bedenk wel dat als je per ongeluk op een website terecht komt die je niet wil zien en je deze onmiddellijk wegklikt, je de website toch zal terugvinden in de Tijdelijke Internet Bestanden (Temporary Internet Files). Dit is dus bijzonder relatief.

[Hoe vaak surfen kinderen gemiddeld op het Internet?](#)

Gemiddeld spenderen kinderen tussen 12 en 18 jaar op een schooldag 2 uur per dag op het internet, op een woensdag 2,5 uur en op een vrije dag (dus ook in het weekend) 3 uur

[Als je internet wil installeren, waar moet je op letten?](#)

Een goede virusscan en een firewall zijn onontbeerlijk bij de installatie van het internet.

[Is het mogelijk om specifieke sites ontoegankelijk te maken? Waar vind ik goede filters?](#)

Er zijn verscheidene filtersystemen op de markt die het mogelijk maken om specifieke websites of websites met bepaalde inhoud te blokkeren. Studies tonen echter aan dat niet alle filtersystemen evenveel veiligheid bieden. Geen enkele filter geeft 100% veiligheid, dus blijft het belangrijk om met kinderen en jongeren te communiceren over het gebruik van de computer en het internet. Het is uw taak als ouder om uw kind bewust te maken van de mogelijkheid dat het schadelijke inhoud tegenkomt en het te leren hoe ze hiermee om te gaan. Bovendien kunnen filters nooit tussenkomen in inhoud die jongeren zelf op het internet plaatsen, zoals via de chat of een blog. Opvoeding blijft dan ook het belangrijkste, filters zijn slechts technische hulpmiddelen.

Wij raden niet één specifieke filter aan. Wij kunnen je wel doorverwijzen naar een site die een vergelijking maakt van filtersystemen in Europa aan de hand van objectieve criteria. Je kan deze informatie vinden op

<http://www.sip-bench.eu/index.html>"<http://www.sip-bench.eu/index.html>

[Kan je websites blokkeren zonder specifieke filtersoftware?](#)

Via de instellingen van je internetbrowser kan je specifieke websites blokkeren. Als je Internet Explorer opent -> Tools-> Internet options -> Security of ->Extra ->Internet opties ->Beveiliging, kan je onder Vertrouwde websites (Trusted) de sites invullen die toegelaten zijn en onder (Restricted) diegene die je wil blokkeren.

Ook hier geldt dezelfde opmerking als voor filtersystemen in het algemeen (zie boven). Aangezien je via dit systeem alle sites die je wenst te blokkeren manueel moet ingeven, is het onmogelijk dat kinderen niet met schadelijke inhoud geconfronteerd worden. Opvoeding én communicatie blijven dus essentieel.

[Hoe werkt parental control?](#)

Er zijn verschillende systemen van parental control op de markt. Deze softwaresystemen laten toe dat ouders bepalen wat kinderen wel of niet kunnen op het internet. Zo kan je websites of programma's blokkeren, tijdsloten instellen die de computer of een applicatie automatisch afsluiten, ... afhankelijk van welk softwaresysteem je gebruikt.

Parental control is eigenlijk een filtersysteem, dus ook hier geldt dezelfde opmerking: het is een technisch hulpmiddel, maar opvoeding en communicatie blijven het belangrijkste (zie boven).

[Is controle enkel mogelijk mits toestemming van mijn kind?](#)

Entertainment (4)

[Hoe lang mag een kind gamen per dag?](#)

Jij als ouder moet degene zijn die bepaalt hoe lang je kind mag gamen, net zoals je bepaalt hoe lang het televisie mag kijken. Bekijk samen met je kind eens welk spel het graag speelt en spreek in het licht daarvan af hoe lang er mag 'gegamed' worden. Het is immers behoorlijk stom om te moeten stoppen met spelen net voor je een nieuwe level bereikt.

[Hoe werkt het delen van bestanden?](#)

Het delen van bestanden (filesharing) gebeurt via een speciale software die maakt dat iemand van op een andere computer toegang heeft tot (een deel van) je harde schijf waardoor hij of zij kan zien wat daarop staat en deze bestanden kan transfereren naar z'n eigen computer. Hiervoor bestaat specifieke software zoals Kazaa, Limewire, Gnutella, ... maar ook via de nieuwe Windows Live Messenger kan je bestanden delen.

[Kan je verslaafd worden aan internet of gamen?](#)

Je kan verslaafd worden aan het internet of games, net als je verslaafd kan raken aan TV kijken, frisdrank drinken, chocolade eten, ... Daarom is het belangrijk dat je van bij het begin duidelijke afspraken maakt rond begin- en einduur van het gamen of internetten. Als ouder heb je de taak om het internetgebruik van je kinderen binnen de perken te houden.

[Hoe vaak surfen kinderen gemiddeld op het Internet?](#)

Gemiddeld spenderen kinderen tussen 12 en 18 jaar op een schooldag 2 uur per dag op het internet, op een woensdag 2,5 uur en op een vrije dag (dus ook in het weekend) 3 uur

Netwerking (20)

[Wat is een goed, onpersoonlijk e-mailadres?](#)

Een veilig e-mailadres is zo neutraal mogelijk (vb. niet sexybabe@hotmail.com) en verklapt niet of je een jongen of een meisje bent. Ook een e-mailadres met voornaam. achternaam is voor kinderen geen goed idee.

[Kan je een bestaand Hotmailadres vernietigen?](#)

Een gratis Windows Live Hotmail-account wordt inactief als je gedurende 120 dagen (4 maanden) of in de eerste 10 dagen nadat je de account hebt aangemaakt niet meer aanmeldt. Als een account inactief is, worden alle berichten, mappen en contactpersonen verwijderd. De accountnaam blijft wel behouden. Deze wordt pas definitief verwijderd als de account 90 dagen inactief is.

Je kan echter ook je account actief afsluiten. Hiervoor meld je je aan op je eigen account, klikt op Help (het vraagtekentje rechts bovenaan). Via het Help-onderwerp "hoe sluit ik mijn account" kan je doorklikken naar een speciale pagina waar je je e-mailaccount kan afsluiten.

[Als je kind het paswoord van zijn e-mailadres niet wil zeggen, is het mogelijk om daar toch achter te komen? Wat met de privacy van mijn kind?](#)

Kinderen hebben recht op privacy. Je kan niet zomaar inbreken in de inbox van je kind, dit valt immers onder het briefgeheim. Tegelijkertijd heb je als ouder de plicht om je kinderen op te voeden. En bij opvoeding hoort nu eenmaal opvolging.

Vertel aan je kinderen dat je samen met hen op regelmatige basis hun inbox wil bekijken. Je kan hun paswoord vragen of hen vragen om hun paswoord in te typen zonder dat u meekijkt.

[Hoe kan ik een e-mail naar een groep mensen sturen zonder dat alle adressen voor iedere ontvanger zichtbaar zijn?](#)

Als je de e-mailadressen van de ontvangers in de lijn Bcc invult (in plaats van Aan of To) zien de ontvangers niet wie de mail nog gekregen heeft. Wanneer je een mail naar verschillende personen verstuurt wordt dit sowieso aangeraden aangezien je in principe geen toestemming hebt om hun e-mailadres naar derden te sturen. Bovendien weet je nooit wat anderen met het e-mailadres van plan zijn.

[Kan ik spam uit mijn mailbox weren?](#)

De meeste e-mailsoftware is uitgerust met een spamfilter waardoor berichten die vermoedelijk ongewenst zijn automatisch in een aparte map terecht komen.

'Spammers' gebruiken vaak computers die het Internet afschuimen, op zoek naar e-mailadressen. Als je e-mailadres op een website gepubliceerd staat, is de kans groter dat je spam ontvangt. De kans op spam verkleint als je in het e-mailadres de @ vervangt door AT of (at). Hierdoor herkennen de zoekcomputers dit niet als een e-mailadres. Ook als je je inschrijft voor nieuwsbrieven, ... wordt de kans op spam groter.

[Hoe omgaan met e-mails die je een gratis gsm of ander cadeau beloven als je de mail naar anderen doorstuurt?](#)

Deze mails zijn vaak spammails of mails die de kettingbrieven van vroeger vervangen. De kans dat je effectief een gsm of een ander cadeau zal ontvangen, is zeer klein, dus je kan deze mail best onmiddellijk deleten en zeker niet doorsturen.

[Doe ik mijn tieners te kort als ik ze verbied om te chatten?](#)

Onze kinderen en jongeren groeien op in een wereld waar computers en het internet deel van uitmaken. Voor hen zijn het geen 'nieuwe' media maar iets dat ze altijd al gekend hebben. Het maakt deel uit van hun wereld en vooral van hun sociale leefwereld. Waar ouders het internet vooral gebruiken om informatie op te zoeken, hebben jongeren de communicatieve kracht ervan ontdekt. Je kan bijna kosteloos urenlang communiceren met je vrienden. Ellenlange chatgesprekken hebben de telefoonconversaties van vroeger vervangen. De chat is naast het rechteekse face-to-facecontact één van de belangrijkste communicatiemiddelen geworden. Kinderen die niet mogen chatten dreigen op de één of andere manier wat sociaal geïsoleerd te geraken.

Vraag eens aan je kind waarom het zo graag chat en je zal zien dat het belangrijk voor hen is. Beter dan het chatten te verbieden zijn het maken van goede afspraken rond wanneer, hoelang, wat kan en wat niet,...

[Wat geef je wel en niet prijs tijdens een chatconversatie?](#)

De gouden regel is en blijft: geef zo weinig mogelijk persoonlijke informatie prijs. Als je chat met vrienden die je ook naast de chat kent, kan je natuurlijk wat meer zeggen. Maar pas op met mensen die je nog nooit ontmoet hebt. Op het internet heb je snel het gevoel dat je iemand kent, dat iemand een goede vriend is. Dit is niet noodzakelijk het geval, dus pas op met wat je zegt tegen iemand die je enkel kent via de chat.

[Hoe kan ik preventief mijn kind beschermen tegen chatverkeer met onbekenden?](#)

Maak met je kind de afspraak dat ze enkel mogen chatten met mensen die ze ook naast de chat kennen. Overloop regelmatig samen hun contactenlijst op MSN en vraag hen wie die mensen zijn en van waar ze ze kennen. Via het internet heb je snel het gevoel dat je iemand kent en kinderen beschouwen iemand waarvan ze het e-mailadres hebben vaak al als 'bekend'. Op de website 'Veiligonline' vind je een demofilmje over de configuratie van MSN zodat er enkel met bekenden kan gechat worden.

[Vanaf welke leeftijd kan ik met mijn kind praten over risico's en gevaren zonder dat ik ze bang maak en dat ze hun vertrouwen in mensen verliezen?](#)

Kinderen tussen 5 en 7 jaar leren het onderscheid te maken tussen goede en kwade intenties. Ze beseffen dat niet iedereen even goede bedoelingen heeft. Gelukkig kunnen ze ook inzien dat niemand helemaal goed of helemaal slecht is.

Kinderen stellen vaak al op heel jonge leeftijd veel vragen over het waarom van gebeurtenissen in hun leven of dingen die ze op televisie zien. Waarom doen mensen dingen die eigenlijk niet mogen? Het is belangrijk dat je je kinderen eerlijk antwoordt op deze vragen. Zo leren ze dat er goede maar ook kwade dingen gebeuren in de wereld.

Leg niet te veel nadruk op de risico's. Maak hen bewust van het feit dat er iets fout kan gaan, maar benadruk tegelijkertijd dat er ook heel veel goede dingen te beleven vallen op het internet en daarbuiten. Leer hen dat ze op hun hoede moeten zijn, maar niet bang hoeven te zijn van alles en iedereen.

[Kan ik een chatroom beveiligen?](#)

Aangezien chatrooms zich op websites bevinden, zijn hier geen beveiligingsinstellingen mogelijk. Dit betekent niet dat het volstrekt onveilig is om hier te chatten. Indien je kind gebruik wil maken van een openbare chatroom, kies dan een chatroom waarop permanent moderators aanwezig zijn. Zo kan je een probleem melden en kan de moderator eventueel onmiddellijk tussenkomen.

[Geeft een elektronische identiteitskaartlezer extra beveiliging?](#)

In principe geeft een elektronische identiteitskaart een extra beveiliging, maar hou in het achterhoofd dat dit slechts relatief is. Je kan immers altijd aanloggen met de identiteitskaart van iemand anders.

[Zijn de instellingen van MSN programma- of persoonsgebonden? Kan je deze veranderen zonder het wachtwoord te kennen?](#)

MSN-instellingen zijn persoonsgebonden. Als verschillende personen een log-in op eenzelfde computer hebben, kunnen hun Messengerinstellingen verschillen. Om iets aan te passen aan de instellingen dien je je aan te melden in het programma voor je iets kan veranderen. Je hebt dus een paswoord nodig.

[Moet je ook toestemming vragen om iemands naam op een website te zetten?](#)

Je moet altijd iemands toestemming vragen om z'n naam, andere persoonsgegevens of foto op een website te publiceren.

[Eens op internet, altijd op internet?](#)

Eens je iets op het internet plaatst, weet je inderdaad niet wat er precies mee gebeurt. Zelfs als je iets verwijdert, zijn er soms nog sporen van terug te vinden. Bovendien kunnen anderen ook altijd foto's, video's of teksten die jij

op het internet zet, opslaan of doorsturen. Je dient dus steeds voorzichtig te zijn welke informatie je op het internet plaatst.

[Kan je makkelijk op een weblog uitkomen zonder de naam van de weblogger te kennen?](#)

Door zijn naam te googelen kom je normaalgezien niet terecht op iemand zijn blog.. De verschillende providers die blogs aanbieden hebben meestal wel een zoekfunctie, maar je kan niet altijd op naam zoeken. Bij Netlog kan dit wel, bij Spaces daarentegen, kan je enkel zoeken op interesses om zo mensen te vinden die in dezelfde dingen geïnteresseerd zijn als jijzelf.

[Hoe kan je weten of je kinderen een weblog hebben aangemaakt?](#)

Vraag het hen. Surf samen met hen eens naar hun blog en bekijk samen wat er op staat.

[Geef je bij een weblog niet altijd persoonlijke informatie door?](#)

Aangezien je op een blog meestal berichtjes zet over wat je interesses zijn, waar je mee bezig bent, wat je aan de wereld wil meedelen, zijn de berichten natuurlijk altijd persoonlijk. En dit is ook niet erg. Wel zet je beter geen persoonsgegevens of contactgegevens op je blog. Deze zijn immers voor iedereen zichtbaar, dus ook voor mensen met minder goede bedoelingen.

[Mag je op een weblog zeggen wat je wilt?](#)

Ook voor weblogs gelden de regels rond vrije meningsuiting. Zaken als racistische, sectarische of discriminerende opmerkingen of andere dingen die bij wet verboden zijn, kunnen ook niet op een weblog. Wat niet strafbaar is, valt meestal onder de wet op de vrije meningsuiting (behalve natuurlijk het publiceren van iemand anders zijn contactgegevens, foto's?...). Iemand die zich geschokt voelt door de inhoud van een weblog, kan eventueel wel contact opnemen met de provider en dit melden. Het is dan aan de provider om af te wegen hoe hij met deze klacht omgaat.

[Wat is het verschil tussen een weblog en een skyblog, een Hi, een Space.... ?](#)

Er zijn verschillende providers die de mogelijkheid aanbieden tot het maken van een weblog of profiel. De meest gebruikte providers zijn Skynet (waar je een skyblog maakt), Spaces (van MSN), MySpace, Netlog, Hi5, Facebook,... Er zijn wel verschillen. Sommige bieden de mogelijkheid aan om muziek, video's, foto's te plaatsen, anderen niet, sommigen hebben een chatfunctie, andere niet, enz...

Cyberpesten (3)

[Kan men inbreken op mijn harde schijf?](#)

"Pas op of ik hack je computer" of "ik blokkeer je MSN" is een dreigement dat vaak door cyberpesters gebruikt wordt. We gaan niet ontkennen dat hacken bestaat, maar je moet al behoorlijk wat kaas gegeten hebben van informatica om hier echt goed in te zijn. Er zijn dus maar weinig mensen die dit effectief kunnen. Zo'n dreigementen zijn dan ook vaak niets meer dan bluf.

Anderzijds denken mensen soms dat er iemand ingebroken heeft in hun computer omdat deze plotseling vreemde dingen doet. Vaak ligt er eerder een virus aan de basis van deze problemen.

[Hoe reageren op cyberpesten?](#)

Bij een geval van cyberpesten is het belangrijk dat er op vijf sporen gewerkt wordt: dader, slachtoffer, omstaanders, ouders en de school. Als ouder is het dan ook het belangrijkste dat je je kind niet beschuldigt of het internet direct verbiedt. Ga na met je kind of het weet wie de dader kan zijn. Vaak is die te zoeken in de schoolcontext. Cyberpesten staat immers nooit echt los van het 'klassieke' pesten. Vaak worden kinderen die slachtoffer worden van cyberpesten ook op de speelplaats geplaagd of gepest. Ga samen met je kind naar de school en bespreek met de leerkracht of directie hoe het probleem kan aangepakt worden.

Veel concrete informatie over signalen of de precieze aanpak van cyberpesten vind je op de website
HYPERLINK www.clicksafe.be

[Kan je ergens klacht indienen tegen illegale inhoud of cyberpesten?](#)

Meldpunt voor racistische inhoud: www.cyberhate.be

Meldpunt voor kinderpornografie: www.stopchildporno.be

De Federal Computer Crime Unit (FCCU) is een onderdeel van de federale politie die zich richt op computercriminaliteit. Bij hen kan je aangifte doen van vermoedelijke misbruiken op het internet of extreme gevallen van cyberpesten. Je kan hiervoor naar de lokale politie stappen, op voorwaarde dat je 'bewijsmateriaal' hebt (printscreens van mail, chatconversatie, datum en uur van het voorval,...). De website van FCCU is www.ecops.be.

Onderwijs (3)

[Mag een school, voetbalclub, vereniging,... foto's of adressen van z'n leerlingen of leden op hun website zetten?](#)

Iedereen heeft een recht van afbeelding. Dat betekent dat je je toestemming moet geven alvorens iemand duidelijk herkenbare foto's van jou mag publiceren of op het internet mag zetten. Bij kinderen die minderjarig zijn moeten in principe ouders hun toestemming geven. Dit geldt zeker voor persoonsgegevens als adressen. Vele scholen of verenigingen fleuren vaak hun website op door foto's te gebruiken, net als jongeren ervan houden om foto's op hun blog te zetten. In principe moet je hier dus steeds toestemming voor vragen. Als de persoon in kwestie vraagt om de foto te verwijderen of om hem of haar onherkenbaar te maken, moet je dit dan ook onmiddellijk doen.

[Kan men nu niet meer studeren zonder computer?](#)

Het internet is een immense bron aan informatie waarop je werkelijk alles snel en gemakkelijk kan terugvinden. Het is dan ook logisch dat het onderwijs van deze technologische evolutie gebruik maakt en van kinderen vraagt om het internet te gebruiken bij het maken van huiswerk. Als dit op een goede manier gebeurt en men bijvoorbeeld het gesprek aangaat rond bronverificatie maakt dit onderdeel uit van de internetopvoeding van kinderen.

[Heeft de school een rol te vervullen in internetopvoeding?](#)

De school heeft als taak om kinderen kennis en vaardigheden bij te brengen zodat ze gewapend zijn om te functioneren in de maatschappij. Deze taak is heel breed en gaat zowel over theoretische dingen, als over rekenen en taal, maar ook bijvoorbeeld verkeersopvoeding waarin we kinderen leren zich op een veilige manier op straat te begeven. Aangezien vandaag ook het internet een onmiskenbaar onderdeel van onze maatschappij uitmaakt, is het een taak van de ouders zowel als de school om kinderen op te voeden tot een veilig en verantwoord internetgebruik.

In Vlaanderen zijn sinds het schooljaar 2007-2008 nieuwe ICT-eindtermen van kracht. Deze eindtermen focussen niet enkel op technische kennis maar ook op het veilig en verantwoord gebruik van Informatie- en CommunicatieTechnologieën.

bron: veiligonline.be