

ICT-groep Broeders Van Liefde

Doel: Opstellen van een gedragscode voor leerlingen en leerkrachten

A. Vertrekpunt: enkele brochures en website

Klikvast, ook op de informatiesnelweg

ICT-vademecum

Het beheer van publieke pc's in de bibliotheek

ICT-competenties

www.saferinternet.be

www.computersindeklas.nl

Vertrekkend met deze achtergrond, bestaande documenten en onze eigen ervaring proberen we (= ICT-coördinatoren) een voorstel tot protocol op te stellen voor computergebruik in de klas. De directies worden hiervan op de hoogte gebracht. In overleg met hen zal een schoolstandpunt en/of een gezamenlijk standpunt ingenomen worden.

A1. Samenvatting Klikvast

Vooraf de cursieve tekst is haalbaar op school- en klasniveau

1. Niet voor kinderoegen bestemd
Om te voorkomen dat kinderen op websites terechtkomen die hinderend zijn geeft de brochure enkele mogelijke technische of pedagogische tips.
 - *Nakijken via monitoring (via geschiedenis)*
 - Filters gebruiken in browser
 - Blokkeren van bepaalde sites
 - Babysit via aangekochte software
 - *Gebruik van kinderbrowsers*
 - *Zelf bibliotheek aanleggen van links*
 - *Overleg met de leerlingen*
2. Veilig, stijlvol en efficiënt communiceren.
Mailen, chatten, sms'en maken deel uit van de jongerencultuur. Ze bieden ruime mogelijkheden voor communicatie en taalvaardigheden. Toch houden ze concrete gevaren in.
 - *Zin en onzin van e-mail: duidelijke afspraken wat kan – wat niet*
 - Gevaren van chat kennen (o.a. misbruik door pedofielen)
of bezoeken via beveiligde sites (zie lijst in de brochure).
Op p. 18 staat een concrete lijst met preventietips en afspraken.
 - Cyberpesten tegengaan (PC afschermen – controle)
 - Bezoek van huiswerksites (Toon in de klas dat je op de hoogte bent. Leer hen het efficiënt te gebruiken.
Tips op p. 20
 - *Regels voor verzorgde en efficiënte communicatie = netetiquette*
Doe aan ethische netetiquette (geen kettingbrieven – gerichte e-mails)
en aan taalkundige netetiquette (afpraak in taalgebruik, onderwerp, toon, humor, hoofdletters).
Tips p. 21
3. Lastige indringers en pottenkijkers
Meer en meer worden we belaagd met virussen, reclame-indringers en spionage. De juiste software installeren is een must.
 - Virussen:
- *voorzorgen nemen dank zij een up-to-date antivirusprogramma.*
- *belangrijke richtlijnen bij lezen van e-mails, downloaden en bij gebruik van diskettes. Tips p. 27*
- *belang van backup nemen onderstrepen.*
 - Spamming (reclame):
- *voorkomen: gepaste software scanner, spaarzaam met je e-mailadres*
- *genezen: toevoegen aan Robinsonlijst (<http://www.robinsonlist.be>) – afzenders blokkeren via software (<http://www.spamfighter.com>)*
 - Netwerkbeveiliging: verstandig omgaan met delen van bestanden – firewall inschakelen – updates van Microsoft uitvoeren -
 - Cookies in- of uitschakelen?
 - Spyware: (spionnen)
- *voorkomen: opletten met freeware programma's – waakzaam zijn*
- *genezen: software:*
4. In bijlage enkele voorbeelden van contracten
 - Toegang tot het lokaal (p. 54)
 - Gebruik van de computers (p. 54)

- Gebruik van het internet (p. 55)
5. Een checklist: Is mijn school cybersafe?
- Schoolbeleid
 - Technische aspecten
 - Internetgebruik
 - Gezond computergebruik (p. 56 – 57)
 - Beveiligingen

A2. Samenvatting: Het beheer van publieke pc's in de bibliotheek

In deze brochure worden een reeks programma's of methodes besproken om de PC te beveiligen.

1. Antivirus en antispyware

- Virussen en worms
- Verschillende gekende merken (p. 38)
- Controleer of het pakket blijft voldoet aan de normen: www.av-test.org of www.virusbtn.com
- Spyware en adware
- Gratis analyse: www.webroot.com/services/spyaudit.htm
- Aanpakken met Ad-aware, Spybot, HijachThis
- Combinatiepakket: Hitmanpro
- Bescherming in realtime: Spywareguard, Spywareblaster, Microsoft Antispyware

2. Systeembeveiliging:

De hele configuratie wordt bevroren.

Via Software

- Deep Freeze
- Skanix Illusion (wordt door verschillende BVL-scholen gebruikt)
- Norton Ghost: maakt een image van de harde schijf

Via Hardware

- Rebornkaart
- HDD-sheriff
- Buitenbeentjes
- Knoppix: opstartgegevens staan op 1 CD. Enkel voor Linux

3. Publieksbrowsers

Ze zorgen ervoor dat de functionaliteit van een PC beperkt blijft. (vb beperkt surfen)

Via software

- WinU
- Quikmenu4windows

Publieksbrowsers voor Microsoft Internet

- Safe Browser (een schil bovenop de browser)
- Teamsoftware (afschermen)
- SiteKiosk (geavanceerde browser combineerbaar met smartcardlezers)
- Microsoft Internet Explorer Administration Kit (je kan de PC naar je hand zetten)

Software voor afscherming van gevaarlijke functionaliteiten

- Verified Security Lockdown
- Spytech Spylock
- Full control

4. Oplossingen voor print-, gebruikers- en tijdsbeheer

Dit probleem is eerder van toepassing in de bibliotheek-wereld, minder op school

A3. Samenvatting website www.saferinternet.be

Een overzichtelijke en praktische website

1. Wanneer

Veilig internetten: een beknopte uitleg

	Informatie	Risico's	Preventie
Surfen	>> lees	>> lees	>> lees
E-mailen	>> lees	>> lees	>> lees
Chatten	>> lees	>> lees	>> lees
Downloaden	>> lees	>> lees	>> lees

Kopen en betalen	>> lees	>> lees	>> lees
Draadloos Netwerk	>> lees	>> lees	>> lees
Overig	>> lees		

Wat kunt u doen om de risico's van het surfen te beperken?

- Wees voorzichtig met het geven van [Persoonlijke gegevens](#)
- Gebruik een goede [Virusscanner](#) en [Firewall](#) om de computer te beschermen.
- Installeer een [Internetfilter](#) om uw kinderen tegen ongewenste inhoud te beschermen
- Installeer een [Popupkiller](#) om het automatisch openen van schermen tegen te gaan.
- Verwijder regelmatig [Cookies](#) van uw computer.
- Scan uw computer regelmatig op [Spyware en Adware](#). Hiervoor zijn goede gratis [programma's](#) te downloaden.
- Meld sites die niet door de beugel kunnen bij de aangewezen [Meldpunten](#).
- [Anoniem Surfen](#).
- Wees alert voor [Dialers](#) die zich ongemerkt op uw computer installeren.

Wat kunt u doen om de risico's van het emailen te beperken?

- [Versleutel](#) uw email en voorkom daarmee dat anderen uw post kunnen lezen.
- Gebruik een goede [Virusscanner](#) met de meest recente virusdefinities.
- Installeer een [Spamfilter](#) of maak gebruik van de faciliteiten die uw provider biedt. Meld ongewenste e-mail bij de OPTA via [Spamklacht.nl](#).
- Reageer nooit op [Spam](#).
- Wees voorzichtig met het openen van bijlagen. Scan deze met de [Virusscanner](#), alvorens te openen.
- Ga nooit in op bedelbrieven van [Nigeriaanse of Zuidafrikaanse oplichters](#), of brieven waarin verzocht wordt uw bankrekening of briefpapier beschikbaar te stellen.
- Ga na wie de werkelijke afzender is door de [Afzender van uw email](#) te achterhalen
- Probeer [Phishing](#) te voorkomen door zeer zorgvuldig om te gaan met het verstrekken van persoonlijke gegevens.
- Gebruik [meerdere e-mailadressen](#) en geef uw belangrijkste e-mailadres alleen aan betrouwbare personen.

Wat kunt u doen om de risico's van het Chatten te beperken?

- Wees tijdens het chatten altijd voorzichtig met het [Vermelden van persoonlijke gegevens](#).
- Praat met kinderen over de risico's van chatboxen en [MSN](#) en volg hun activiteiten.
- Bescherm uw computer tegen [Autodialers](#)
- Wees alert op [Pesten](#) en meldt dit aan de chatbox moderator
- Spreek bij ontmoetingen met een onbekende af in een openbare gelegenheid en neem bij voorkeur iemand mee.
- Veel mensen maken op internet gebruik van een pseudoniem, in de vorm van een 'nickname' of een alias. Het is voor (privé) personen op internet zo volkomen normaal en geaccepteerd om een pseudoniem te gebruiken, dat het deel is gaan uitmaken van de internetcultuur.

Wat kunt u doen om de risico's bij het delen downloaden van bestanden te beperken?

- Gebruik een goede [Virusscanner](#) om de gedownloadde bestanden te scannen.
- Bied geen bestanden met illegale inhoud aan.
- Gebruik alleen programma's waarvan bekend is dat ze geen [spyware/adware](#) bevatten
- Verwijder de [Windows Scripting Host](#) en sluit de computer voor het [delen van bestanden en printers](#) (geldt voor Windows versies 96 98 en ME)
- Voor de nieuwere Windows versies is een goede [Firewall](#) onmisbaar.

Wat kunt u doen om de risico's van een draadloos netwerk te beperken?

- Gebruik versleuteling. Indien beschikbaar is WPA (Wi-Fi Protected Access) de beste methode. Zo niet gebruik dan de sterkst beschikbare versie van WEP (Wired Equivalent Privacy).

- Als iemand uw netwerk langere tijd gericht kan bestuderen, bijvoorbeeld iemand die in de buurt woont, kan WEP encryptie worden doorbroken.
Vervang daarom regelmatig de WEP sleutels.
- Schakel ongebruikte draadloze apparatuur uit.

2. Voor wie Doelgroepen van SurfopSafe

	Informatie	Tips	Links
Kinderen	>> lees	>> lees	>> lees
Ouders	>> lees	>> lees	>> lees
Docenten	>> lees	>> lees	>> lees
Senioren	>> lees		>> lees
Bedrijven	>> lees	>> lees	>> lees

3. Risico's SurfopSafe de risico's

Op de risico-pagina's leest u welke risico's u kunt lopen bij het internetten. Ze zijn in zes hoofdgroepen onderverdeeld. Per hoofdgroep vermelden we het soort risico, wat u ter preventie kunt doen, wat u moet doen als er toch iets mis gaat en wat het overheidsbeleid is inzake risico's. U kunt in onderstaande tabel direct doorklikken naar de pagina van uw keuze of de informatie per risico bekijken.

	Informatie	Preventie	Crisis	Beleid	Links
Virussen	>> lees	>> lees	>> lees	>> lees	>> lees
Hackers	>> lees	>> lees	>> lees	>> lees	>> lees
Spam	>> lees	>> lees	>> lees	>> lees	>> lees
Fraude	>> lees	>> lees	>> lees	>> lees	>> lees
Privacy	>> lees	>> lees	>> lees	>> lees	>> lees
Ongewens contact	>> lees	>> lees	>> lees	>> lees	>> lees

B. Enkele modellen voor afspraken

B1. Internetprotocol van surfopsafe

1. Op het internet gebruik ik alleen mijn voornaam. Andere persoonlijke gegevens zoals foto's, achternaam, adres en telefoonnummer houd ik voor mijzelf. Het adres en telefoonnummer van de school geef ik alleen door na toestemming van de juf of de meester.
2. Ik maak via internet geen afspraken met onbekenden.
3. Bij het gebruik van een zoekmachine, bijvoorbeeld IIs of Google, gebruik ik nooit zoekwoorden die te maken hebben met seks, discriminatie, geweld of grof taalgebruik.
4. Chatten of MSN-en is op school niet toegestaan.
5. Als ik op internet vervelende informatie tegenkom, waarschuw ik direct de juf of de meester.
6. Downloaden van bestanden mag alleen met toestemming van de juf of de meester.
7. Aan de instellingen van de computer, bijvoorbeeld screensavers, mag door mij niets worden veranderd.
8. Printen doe ik alleen met toestemming van de meester of de juf.
9. Ik gebruik geen scheldwoorden als ik een email verstuur. Ik zal nooit antwoorden op vervelende mailberichten die te maken hebben met seks, geweld, racisme of mensen die mij iets willen verkopen. Vervelende mails laat ik aan mijn meester of juf zien zodat zij actie kunnen ondernemen.
10. Door dit protocol te ondertekenen beloof ik me aan deze afspraken te houden.

B2. Netiquette voor het voortgezet onderwijs van surfopsafe

Het woord 'Netiquette' is een samenvoeging van netwerk en etiquette. Of anders gezegd: de gedragsregels voor internet. Vaak wordt er door internetgebruikers vergeten dat we via internet met mensen en niet met machines communiceren. Deze richtlijnen helpen ons het internet leuk te houden en de communicatie tussen mensen zo prettig mogelijk.

1. Denk aan de mens achter de computer.
2. Gedraag je op internet niet anders dan je in het gewone leven zou doen.
3. Respecteer de privacy van anderen en ga daar altijd zorgvuldig mee om.
4. Respecteer altijd de mening van een ander. Reageer zonnodig zakelijk en voorkom ordinaire ruzies.
5. Bedenk bij het verzenden van een bericht of de inhoud voor de ontvanger interessant is.
6. Ga niet rondneuzen in anderma ns computer.
7. Bedenk dat alles wat je intikt of op het web zet opgeslagen wordt en dus, zelfs jaren later, weer te voorschijn kan komen.
8. Respecteer copyright: vermeld, wanneer je materiaal van internet overneemt, waar het vandaan komt.
9. Zorg dat de informatie die je via het web aanbiedt legaal is. Verzend of download nooit illegale software of bestanden.
10. Meld sites of mails die niet door de beugel kunnen, bijvoorbeeld op het gebied van kinderporno, racisme of discriminatie bij de daarvoor bestemde meldpunten.

Blijf meewerken aan een veilig en prettig internet voor iedereen!

B3. Enkele voorbeelden van contracten in Klikvast

Toegang tot het lokaal (p. 54)
Gebruik van de computers (p. 54)
Gebruik van het internet (p. 55)

B4. Een checklist in Klikvast: Is mijn school cybersafe?

Schoolbeleid
Technische aspecten
Internetgebruik

B5. Concrete tips in Klikvast

Op p. 18 staat een concrete lijst met preventietips en afspraken.

Op p. 20 bezoek aan huiswerksites

Op p. 20: Regels voor verzorgde en efficiënte communicatie = netetiquette

Op p. 21: en aan taalkundige netetiquette (afspraak in taalgebruik, onderwerp, toon, humor, hoofdletters).

C. Afspraken:

Op de komende vergadering zullen we hieruit een keuze maken.

C1: Software

Welke software als beveiliging op welke PC?

C2: Gebruik door leerlingen

Algemene afspraken (= soort contract)?

Wat is niet toegelaten?

Wat wordt toegelaten?

Wat is toegelaten mits controle?

Welke sanctie bij overtreding?

C3: Gebruik door leerkrachten

Algemene afspraken (= soort contract)?

Wat is niet toegelaten?

Wat wordt toegelaten?

Wat is toegelaten mits controle?

Welke sanctie bij overtreding?

Goede moed,

Asper, 27 januari 2005

marcdewaele@telenet.be