



Regeling gebruik elektronische informatie- en communicatiemiddelen

(Regeling EIC-middelen)

Ede, oktober 2010

Regeling gebruik elektronische informatie- en communicatiemiddelen

Artikel 1: Doel en werkingssfeer van deze regeling

- Lid 1: Deze regeling geeft de wijze aan waarop binnen vereniging CNS en de CNS-scholen wordt omgegaan met elektronische informatie- en communicatiemiddelen (EIC). Deze regeling omvat gedragsregels ten aanzien van verantwoord gebruik en geeft regels over de wijze waarop controle plaats vindt.
- Lid 2: Onverantwoord gebruik is gebruik tegenstrijdig aan de doelstelling en identiteit van de vereniging, zowel in persoonlijk gebruik als in relatie tot anderen binnen of buiten de CNS-scholen. Hierbij wordt in het bijzonder gedacht aan illegale toepassingen van bestanden, godslasterlijke, beledigende, aanstootgevende, gewelddadige, racistische, discriminerende, intimiderende, pornografische toepassingen, zinloos tijdverdrijf en /of toepassingen die strijdig zijn met de wet of als onethisch te karakteriseren zijn.
- Lid 3: De controle op persoonsgegevens bij gebruik van elektronische informatie- en communicatiemiddelen vindt plaats met als doel:
- a. systeem- en netwerkbeveiliging
 - b. tegengaan onverantwoord gebruik.
- Lid 4: Deze regeling geldt voor een ieder die ten behoeve van de CNS-scholen en het bestuursbureau werkzaamheden verricht.

Artikel 2: Algemene uitgangspunten

- Lid 1: De controle op het gebruik van elektronische informatie- en communicatiemiddelen zal overeenkomstig deze regeling worden uitgevoerd.
- Lid 2: Gestreefd wordt naar een goede balans tussen controle op verantwoord gebruik en bescherming van de privacy van personeelsleden op de werkplek.
- Lid 3: Vereniging CNS treft voorzieningen t.b.v. de positie en integriteit van de systeembeheerder. Dit wordt geconcretiseerd door de bovenschoolse staffunctionaris ICT alleen technisch verantwoordelijk te laten zijn. Dit laat onverlet het bepaalde in artikel 5.5.

Artikel 3: Gebruik van elektronische informatie- en communicatiemiddelen

- Lid 1: Het gebruik van elektronische informatie- en communicatiemiddelen is primair verbonden met taken/bezigheden die voortvloeien uit de functie van het personeelslid. E-mail communicatie heeft slechts plaats via het schoolaccount. Voor personeelsleden en voor ouders met een vertrouwensfunctie vindt e-mailcommunicatie slechts plaats via een schoolaccount. Gedragsregels die gelden voor het ondertekenen van schriftelijke correspondentie, het vertegenwoordigen van de CNS-scholen en het bestuursbureau en op het verzenden van post, zijn ook van toepassing op gebruik van elektronische informatie- en communicatiemiddelen.
- Lid 2: Personeelsleden mogen elektronische informatie- en communicatiemiddelen beperkt, incidenteel en kortstondig gebruiken voor persoonlijke doeleinden, mits dit niet storend is voor de dagelijkse werkzaamheden of het systeem en mits hierbij wordt voldaan aan de verdere regels van deze regeling.
- Lid 3: Het is niet toegestaan om elektronische informatie- en communicatiemiddelen zodanig te gebruiken dat het systeem- en/of de beveiliging opzettelijk worden aangetast, of de inhoudelijke communicatie tegenstrijdig is aan de doelstelling en identiteit zoals omschreven in artikel 1.2.

Lid 4: Het is niet toegestaan om elektronische informatie- en communicatiemiddelen voor onacceptabele doeleinden te gebruiken. Hierbij moet onder andere worden gedacht aan het spelen of downloaden van niet educatieve spelletjes, winkelen, gokken of deelnemen aan kansspelen, en het bezoeken van niet educatieve chatboxen .
Het elektronisch contact tussen leerkracht en leerlingen al dan niet in privé – tijd is alleen toegestaan als dit in een beveiligde, afgeschermdde omgeving plaatsvindt. De communicatie heeft als doel om schoolse zaken te bespreken. Voor deze communicatie is altijd toestemming van de betreffende ouder(s) nodig.

Lid 5: **Het is in het bijzonder niet toegestaan om:**

- bewust sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten;
- bewust pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal te bekijken of te downloaden of te verspreiden;
- bewust informatie waartoe men via elektronische informatie- en communicatiemiddelen toegang heeft verkregen zonder toestemming te veranderen of te vernietigen;
- actief aan te geven aan webwinkels dat belangstelling bestaat voor het ontvangen van productinformatie voor eventuele latere bestellingen in de privé-sfeer;
- bestanden te downloaden die geen verband houden met studie en/of werk;
- software en applicaties te downloaden zonder voorafgaande toestemming van de beheerder;
- niet-educatieve spelletjes te spelen;
- anoniem of onder een fictieve naam via elektronische informatie- en communicatiemiddelen te communiceren;
- op dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende manier via elektronische informatie- en communicatiemiddelen te communiceren;
- inkomende privé-berichten te genereren door het deelnemen aan niet-zakelijke nieuwsgroepen, abonnementen op e-zines, elektronisch winkelen, down- en uploaden van bestanden, nieuwsbrieven en dergelijke;
- kettingmailberichten te verzenden of door te sturen;
- een mobiele telefoon van de school te gebruiken in het buitenland zonder uitdrukkelijke toestemming van het bevoegd gezag;

Lid 6: Het is niet toegestaan om foto's, video's of ander materiaal van op CNS-scholen of op het bestuursbureau werkzame personen of leerlingen of andere bij de CNS-scholen betrokkenen via elektronische informatie- en communicatiemiddelen bekend te maken. Voor het bekend maken van foto's waarop personen zijn afgebeeld is voorafgaande toestemming van betrokkene of diens wettelijke vertegenwoordiger vereist.

Lid 7: Het is ook anderszins niet toegestaan om door middel van elektronische informatie- en communicatiemiddelen onethisch te handelen.

Lid 8: User-identificatie (gebruikersnaam) en authenticatie (bijvoorbeeld wachtwoord) zijn persoonsgebonden en mogen niet aan anderen worden doorgegeven.

Lid 9: Onbedoelde inbreuken op beveiliging, van binnenuit of van buiten de CNS-scholen of het bestuursbureau dienen onmiddellijk aan de bovenschoolse staffunctionaris ICT gemeld te worden.

Artikel 4: Meldingsplicht

Lid 1: Een vermoeden van misbruik van elektronische informatie- en communicatiemiddelen moet direct worden gemeld bij de schoolleiding of de algemeen directeur.

Artikel 5: Controle

- Lid 1: Controle op gebruik van elektronische informatie- en communicatiemiddelen vindt slechts plaats in het kader van in artikel 1.2 en 1.3 genoemde doelen.
- Lid 2: De personeelsleden worden voorafgaand aan de invoering van de regeling geïnformeerd over controle op elektronische informatie- en communicatiemiddelen, omtrent de doeleinden, de aard van de gegevens, de omstandigheden waaronder zij verkregen zijn en de inhoud van deze regeling.
- Lid 3: Niet toegestaan gebruik van elektronische informatie- en communicatiemiddelen wordt zo veel mogelijk technisch onmogelijk gemaakt.
- Lid 4: Controle vindt in beginsel steekproefsgewijs plaats.
- Lid 5: Als een lid van de schoolleiding, de algemeen directeur of de bovenschoolse staffunctionaris ICT merkt of er op geattendeerd wordt dat het EIC-gedrag van een personeelslid niet binnen deze kaders verloopt, wordt de collega hier op gewezen en wordt een controle van zijn EIC-acties door bevoegde personen als mogelijkheid genoemd.
- Lid 6: Elektronische informatie- en communicatieberichten van de (bovenschoolse) schoolleiding, bestuursleden, vertrouwenspersonen en andere personeelsleden met een vertrouwensfunctie, gecommuniceerd in het kader van hun functie, zijn in beginsel uitgesloten van controle. Dit geldt niet voor de controle bij een ernstig vermoeden van misbruik.
- Lid 7: De geanonimiseerde rapportage wordt verstrekt aan de (bovenschoolse) schoolleiding en aan de bovenschoolse staffunctionaris ICT. De (bovenschoolse) schoolleiding kan naar aanleiding van deze rapportage vragen om een gepersonaliseerde rapportage.
- Lid 8: Indien een personeelslid of een groep personeelsleden ervan wordt verdacht de regels te overtreden, kan gedurende een vastgestelde (korte) periode gerichte controle plaatsvinden. De schoolleiding meldt dit aan het bestuur.
- Lid 9: Het bestuur geeft indien nodig aan de bovenschoolse staffunctionaris ICT de opdracht om de elektronische informatie- en communicatiemiddelenacties van de betrokkene na te gaan.
- Lid 10: De bovenschoolse staffunctionaris ICT brengt hiervan schriftelijk verslag uit aan het bestuur.
- Lid 11: Personeelsleden, ten aanzien van wie geconstateerd is dat zij zich niet aan deze regeling houden, worden zo spoedig mogelijk door de leidinggevende op hun gedrag aangesproken.
- Lid 12: Bij handelen in strijd met deze regeling beslist het bestuur over de al dan niet te nemen (disciplinaire) maatregelen. Tot deze maatregelen kan ontslag uit het dienstverband behoren.

Artikel 6: Inwerkingtreding

De regeling gebruik informatie- en communicatiemiddelen is vastgesteld door het bevoegd gezag en treedt in werking op d.d. 1 november 2010.

Toelichting op de EIC- modelregeling

De EIC-modelregeling betreft het gebruik van (mobiele) telefoon, internet, e-mail en andere huidige en toekomstige elektronische informatie- en communicatiemiddelen zoals deze ter beschikking worden gesteld of worden gefinancierd door uw werkgever. In de tekst wordt hiernaar in algemene zin verwezen als "*elektronische informatie- en communicatiemiddelen*".

Een aantal organisaties voor bestuur en management in het PO en VO, te weten Besturenraad, Bond KBO en Bond KBVO, VBS en VGS, heeft gezamenlijk de voorliggende modelregeling opgesteld.

Een belangrijk punt is de totstandkoming van een goede balans tussen verantwoord gebruik van deze elektronische informatie- en communicatiemiddelen en bescherming van de privacy van iedereen die op CNS-scholen of het bestuursbureau werkzaamheden verricht en achter de pc zit (dus ook vrijwilligers, stagiaires, enz.). De tekst van de modelregeling sluit op dat punt aan bij de Wet bescherming persoonsgegevens (Wbp).

Belangrijk is dat de Wbp alleen geldt als er sprake is van persoonsgegevens. Gegevens met betrekking tot bijvoorbeeld e-mail- en internetgebruik van personeel zijn in het algemeen te kwalificeren als persoonsgegevens.

Een specifieke brochure over internetgebruik op de werkplek is bij het College Bescherming Persoonsgegevens op te vragen.

Het model is **niet** van toepassing op het gebruik van elektronische informatie- en communicatiemiddelen door leerlingen. Zie hiervoor het schoolgebonden multimedia protocol.

Op grond van art. 7:660 BW is de werkgever gerechtigd tot het geven van voorschriften voor het verrichten van de arbeid en het nemen van maatregelen ter bevordering van de goede orde in de onderneming (in dit geval op de CNS-scholen en het bestuursbureau).

Gebaseerd op dit artikel gaat de werkgever over tot het reguleren en controleren van e-mail en internet. Vereniging CNS kiest ervoor een reglement op te stellen waarin afspraken zwart op wit worden gezet over met name internet en e-mailgebruik. Daarin leggen Vereniging CNS en het personeel schriftelijk vast wat wel en wat niet kan. Op deze manier legt de Vereniging vast tot hoever deze zal gaan bij het maken van inbreuken op de privacy van op CNS-scholen en het bestuursbureau werkzame personen. De personeelsleden van de vereniging hebben hierdoor een houvast hoe vaak en op welke manier ze internet en e-mail gebruiken kunnen.

Uit rechterlijke uitspraken is op te maken dat er veel waarde wordt gehecht aan het hebben van een reglement of protocol, dit is voor Vereniging CNS dan ook aanleiding geweest een reglement te willen vaststellen.

Communicatieplan:

Alle personeelsleden die binnen de vereniging werkzaam zijn worden over de inhoud van de regeling geïnformeerd door de regeling aan alle personeelsleden op papier en/of via e-mail te sturen, door publicatie in een personeelsnieuwsbrief, bij het uitreiken van een e-mailadres of een nieuwe mobiele telefoon e.d. Daarnaast zal het reglement worden opgenomen in de introductiemap nieuwe medewerkers.

Artikelsgewijze toelichting

Artikel 1: Doel van deze regeling

Deze regeling is van toepassing op personen in dienst van of werkzaam voor vereniging voor Christelijk Nationaal Schoolonderwijs te Ede en omgeving: zij die ten behoeve van de CNS-scholen of het bestuursbureau werkzaamheden verrichten. Hieronder vallen niet alleen de personen die een akte van benoeming/aanstelling hebben, maar ook uitzendkrachten, stagiaires, vrijwilligers, personen die bij de CNS-scholen of het bestuursbureau zijn gedetacheerd, etc. In de tekst wordt geregeld het woord personeelslid gebruikt maar hier worden dus alle personen bedoeld die in dienst van of werkzaamheden ten behoeve van de vereniging verrichten.

Artikel 2: Algemene uitgangspunten

Lid 3:

De maximale bewaartermijn van 6 maanden geldt specifiek in het kader van deze regeling; relevante informatie die opgenomen dient te worden in een (personeels)dossier, valt onder de werking van de Wbp en kan uit dien hoofde langer worden bewaard. Als er bijvoorbeeld naar aanleiding van een controle reden is om met een personeelslid in gesprek te treden, een waarschuwing te geven, etc. zal dit uiteraard in het personeelsdossier worden vastgelegd (zie ook artikel 5).

Lid 4:

In deze regeling is ervoor gekozen de bovenschoolse staffunctionaris ICT enkel een technische, signalerende verantwoordelijkheid toe te delen. Daarmee kan worden voorkomen dat hij/zij in een loyaliteitsconflict komt met één van zijn collega's. Bij een vermoeden van misbruik van de EIC-middelen van de CNS-scholen of het bestuursbureau wordt het desbetreffende personeelslid door of namens de schoolleiding of de algemeen directeur hierop gewezen (zie ook artikel 5.5. van de modelregeling).

Omdat de bovenschoolse staffunctionaris ICT toegang heeft tot bijna alle gegevens binnen het computernetwerk moet deze functie met de nodige waarborgen omgeven zijn. Zo heeft hij/zij, net als overigens al het personeel maar op grond van de aard van zijn/haar werkzaamheden in het bijzonder, een geheimhoudingsplicht. Ook is hij/zij niet bevoegd tot het lezen van e-mail of het real-time meekijken zonder dat daartoe een aanleiding is. De bovenschoolse staffunctionaris ICT moet tegenover de (boven)school(se) leiding of het bestuur een zekere onafhankelijkheid hebben. Hij/zij mag niet door de (boven)school(se) leiding of het bestuur gedwongen worden af te wijken van procedures die de zorgvuldigheid van het proces bewaken.

Artikel 3: Gebruik van elektronische informatie- en communicatiemiddelen

Een totaal verbod op het privégebruik van elektronische informatie- en communicatiemiddelen zoals het versturen en ontvangen van persoonlijke e-mailberichten is niet reëel. De vereniging heeft daarom wel een aantal beperkende voorwaarden vastgesteld t.a.v. het privégebruik.

In de regeling zijn gedragsregels opgenomen over wat er binnen de vereniging onder bijvoorbeeld verantwoord e-mailgebruik wordt verstaan: Deze zijn;

- een correcte vermelding van afzender;
- het meesturen van een disclaimer;
- duidelijke onderwerpaanduiding;
- terughoudend omgaan met vertrouwelijke gegevens en gevoelige informatie.

Voorbeelden van niet toegestaan gebruik zijn:

- het versturen en ontvangen van kettingbrieven;
- het versturen van e-mailberichten met een dreigende inhoud.

Als de inhoud van een e-mail in ernstige mate ontoelaatbaar is (opruiend, hatelijk, onsmakelijk etc.), of de wet overtreedt (bijvoorbeeld door valse beschuldigingen te doen), neemt de vereniging contact op met de politie. De e-mail wordt dan uitgeprint en een (digitale) kopie als potentieel bewijsmateriaal zal worden bewaard. Let op: het adres waar een e-mail vandaan komt is te vervalsen, dus de werkelijke afzender kan zijn/haar identiteit onder iemand anders' naam verborgen houden.

Telewerken is niet apart vermeld in deze regeling. De controle door de werkgever van het computergebruik van het personeel vormt in situaties waarin het personeelslid vanuit zijn eigen huis inlogt op het computersysteem van de CNS-scholen of het bestuursbureau (telewerken) een extra probleem. Voor zover het personeelslid uitsluitend ten behoeve van het werk inlogt, zullen de regels in deze regeling van overeenkomstige toepassing zijn. De computer van het personeelslid thuis maakt dan immers logisch gezien deel uit van het computernetwerk en het personeelslid bevindt zich in een situatie waarin ook de gezagsbevoegdheid van de werkgever geldt.

Dit is anders als het personeelslid de schoolaccount kan en mag gebruiken om privé e-mail te versturen of om in zijn eigen tijd over het internet te surfen. Voor logging van hetgeen hij privé doet, is veelal geen grond. Dit geldt zeker indien ook zijn gezinsleden van de faciliteiten gebruik mogen maken. Met hen heeft Vereniging CNS als werkgever immers geen arbeidsrelatie, waarin hij zijn gezag kan uitoefenen. Zijn positie is in deze situatie vergelijkbaar met een provider.

Het personeel wordt verzocht niet te antwoorden op junkmail, omdat de kans groot is dat men er nog meer van ontvangt als men het wel doet. Daarnaast is voorzichtigheid geboden met het bekend maken van het e-mailadres op websites. Ook bij het invullen van het huisadres in publieke gebieden, zoals bijvoorbeeld een 'gastenboek', is voorzichtigheid geboden. E-mailberichten waar grote bestanden als attachment zijn toegevoegd, met name als ze afkomstig zijn van mensen die men niet kent of met onderwerptitels die niets zeggen, worden direct verwijderd. Verwijder bovendien ieder verdacht bericht en leeg aansluitend prullenbak van de e-mailbox.

Artikel 5: Controle

De werkgever is verplicht om het personeel, maar ook uitzendkrachten, stagiaires, vrijwilligers, personen die bij de CNS-scholen of het bestuursbureau zijn gedetacheerd inlichtingen te verschaffen over het doel van de controlemiddelen, de manier waarop de gegevens worden verkregen en het gebruik dat ervan wordt gemaakt. Transparantie is een belangrijk beginsel voor privacybescherming. De informatieplicht is -afhankelijk van de situatie- gebaseerd op de artikelen 33 en 34 WBP. De verplichting vloeit ook voort uit de Arbowetgeving. Het enkele overleg met de (G)MR is in dit kader onvoldoende. Het personeel moet individueel worden voorgelicht. In geval van e-mail- en internetcontrole is het moment van inloggen hiervoor het aangewezen tijdstip.

Het personeelslid heeft het recht op inzage in de gegevens. Hij kan verder de werkgever verzoeken de gegevens aan te vullen, te verbeteren, te verwijderen of af te schermen indien deze feitelijk onjuist zijn, voor het doel onvolledig of niet ter zake dienend zijn dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt. Tenslotte kan het personeelslid tegen de verwerking van zijn persoonsgegevens verzet aantekenen in verband met zijn bijzondere persoonlijke omstandigheden.

Lid 9, lid 11 en lid 13

Via het managementstatuut kan dit gemandateerd worden aan de (bovenschoolse) schoolleiding.

Lid 9

Als er een vermoeden is op grond waarvan een gepersonaliseerde controle plaatsvindt, wordt de algemeen directeur hierover geïnformeerd. (zie artikel 5.9).

Zie ook de toelichting bij artikel 2 lid 3.

Verklarende begrippenlijst:

Aanbieder (ISP/Internet Service Provider): bedrijf dat de toegang tot het internet aanbiedt, zoals bijvoorbeeld Xs4all, Chello, en Planet. Letterlijk: verschaffer of verlener.

Attachment (bijlage): letterlijk toevoeging; een bestand dat wordt gekoppeld aan een e-mailbericht. De aanwezigheid van een attachment is zichtbaar door een paperclipsymbool naast het bericht.

Babbelbox: ontmoetingsplaats voor mensen die met behulp van elektronische middelen met elkaar communiceren. Ook wel chatbox genoemd.

Browser: afkorting voor Web Browser. Dit is het programma dat de gebruiker in staat stelt over het web te 'surfen'. De populairste webbrowsers zijn Netscape Navigator en Internet Explorer.

Cache: extra, snel aanspreekbaar geheugen, bedoeld voor het opslaan van veelgebruikte computeropdrachten, waardoor ze sneller beschikbaar zijn.

Chatbox: ontmoetingsplaats voor mensen die met behulp van elektronische middelen met elkaar communiceren. Ook wel babbelbox genoemd.

Chatroom: plekken op internet waar mensen naartoe gaan om met anderen te kletsen ('chatten') in een virtuele kamer. Deze kamers zijn over het algemeen ingedeeld per onderwerp, zodat iedere gebruiker kan kletsen met iemand die dezelfde interesse deelt. Als men zich in een chatroom bevindt, kan men alle gesprekken die plaatsvinden in één keer op het scherm zien.

Cookie: een klein tekstbestand dat door sommige sites op de harde schijf van de pc wordt gezet. Het bevat door de gebruiker opgegeven informatie, zoals voorkeuren of e-mailadres. Als men de site later weer bezoekt, hoeft men niet weer dezelfde vragen te beantwoorden. Het bestand kan gebruikt worden om de gebruiker te volgen en surfgedrag bij te houden op het Web.

Datalimiet: maximale hoeveelheid data die gedownload mag worden.

Disclaimer: letterlijk uitsluiting van verantwoordelijkheid. Disclaimers verschijnen vaak onderaan e-mailberichten of webpagina's. Hierin wordt de lezer er op geattendeerd dat aan de uitspraken geen rechten ontleend kunnen worden.

Domeinnaam: de tekst waarmee een specifieke (internet-)host wordt aangeduid. Domeinen zijn grote gebieden die per doel of soort organisatie verdeeld worden (.com voor commercie, .edu voor onderwijs, gov. voor overheid, org. Voor non-profit, enzovoort).

Download: gegevenstransport van het internet naar een computer. Ook gegevenstransport tussen computer en printer of tussen twee computers.

E-mail: elektronische post. Het stelt de gebruiker in staat berichten over het internet te versturen en te ontvangen.

E-zine: electronic magazine, tijdschrift in elektronische vorm, dat verspreid wordt via e-mail.

Fair Use Policy: de afspraak met een provider dat geen excessief gebruik gemaakt wordt van de verbinding.

FAQ: afkorting van Frequently Asked Questions, hetzelfde als Veel Gestelde Vragen. Om niet telkens alle vragen te hoeven beantwoorden, worden veel voorkomende vragen en bijbehorende antwoorden in een apart bestand gezet.

Favorieten: ook wel bookmarks genoemd. Dit zijn opgeslagen verwijzingen naar websites. Ze stellen de gebruiker in staat zonder omwegen terug te keren naar iedere site, zonder het adres opnieuw in te hoeven typen.

Filteren: hardware of software, ontworpen om bepaalde informatie, zoals porno, geweld en racisme te blokkeren.

Firewall: veiligheidsvoorziening. Bij het kopiëren van bestanden van een andere computer naar de eigen computer kunnen ook virussen binnengehaald worden. Om dat te voorkomen is een firewall een beschermingsmogelijkheid. Het is een beveiliging tussen het externe (internet) en het interne netwerk (LAN), die probeert te voorkomen dat onbevoegden toegang krijgen tot het interne netwerk. Men kan wel van binnen naar buiten gaan, maar niet andersom.

Freeware: gratis software die van internet afgehaald kan worden en die gebruikt mag worden, mits er niets aan veranderd wordt. Er rust copyright op. De software mag niet commercieel verhandeld worden.

FTP: afkorting van File Transfer Protocol, het meest gebruikte standaardprotocol om bestanden te versturen of te ontvangen. Het bestand kan software, tekst, beeld, video of geluid zijn. Na het opgeven van naam en wachtwoord kunnen bestanden verstuurd (upload) worden of ontvangen (download) worden.

Gebruikersnaam: de naam waarmee men zich op internet meldt. Ook wel username of login genoemd.

Hacken: term gebruikt voor het inbreken in computers computernetwerk door het kraken van beveiligingen om aan te tonen dat computers nog lang niet veilig zijn. Hackers proberen via internet netwerken binnen te dringen.

Hoax: een hoax (spreek uit: hooks) is een internetterm voor een loze of valse waarschuwing of een verzonden verhaal over virussen en trojan horses. Eindeloos verspreid door goedbedoelende internetgebruikers, waardoor een hoax zich min of meer hetzelfde gedraagt als een virus.

Host: letterlijk gastheer. Een host is een centrale computer die grote hoeveelheden gegevens bevat die door meerdere terminals kunnen worden benaderd. De host is door vaste lijnen te koppelen aan terminals, maar kan ook gekoppeld worden aan computers via tijdelijke verbindingen. de computer ('server') waarop een website fysiek is gelokaliseerd.

HTML: afkorting voor HyperText Mark-up Language. HTML is de programmeertaal waardoor het internet werkt. HTML is een zogenaamde onderscheidingstaal. Het heeft de taak de bestanddelen van een document te beschrijven. HTML bevat opdrachten voor het markeren van documentelementen, zoals kopstukken, tekstgedeeltes, lijsten, tabellen of grafische referenties, uitgaande van een hiërarchische deling.

Hyperlink: een link zorgt ervoor dat men met slechts één muisklik van de ene naar de andere internetsite gaat. Links kunnen bestaan uit een tekst of een afbeelding. Tekstlinks zijn meestal onderstreept en hebben vaak een kleur die afwijkt van de rest van de tekst. Afbeeldinglinks kunnen plaatjes, tekeningen of animaties zijn. Op een link verandert de muisaanwijzer meestal in een handje. De link is in feite het internetadres waarheen verwezen wordt.

ICQ: kort voor I Seek You - ik zoek je. Programma dat gebruikt kan worden om te kijken of er bekenden online zijn. Zij moeten dan ook ICQ gebruiken.

ICT: afkorting van Informatie- en CommunicatieTechnologie. Gebruikt voor alles wat te maken heeft met automatisering en telecommunicatie.

IP: afkorting van Internet Protocol. De op internet gehanteerde taal om gegevens uit te wisselen. Met deze taal kan een computer precies aangeven naar welk adres de informatie toe moet.

IRC: afkorting van Internet Relay Chat. IRC is voor internetgebruikers een manier om met elkaar over allerlei onderwerpen te praten. Oneerbiedig wordt IRC ook wel de babbelbox van internet genoemd. Soms zijn de discussies door iedereen te volgen, soms niet. De gesprekken zijn altijd realtime. Dat wil zeggen, voor de één kan het zeven uur 's morgens, voor de ander kan het twee uur 's nachts zijn. Het is een van de populairste toepassingen van internet. Ook is er een heel apart jargon ontstaan bij IRC'ers.

ISP: afkorting van Internet Service Provider. Organisatie die via eigen servers andere organisaties en privé-gebruikers toegang biedt tot internet.

LAN: afkorting van Local Area Network, computernetwerk binnen een beperkt gebied, bijvoorbeeld binnen een gebouw of een universiteitscomplex. De aangesloten gebruikers delen ook printers en andere apparatuur.

Modem: modems zorgen ervoor dat informatie van de ene computer naar de andere kan worden overgedragen via elke telefoonlijn.

Nieuwsgroepen: dit zijn elektronische discussiegroepen voor mensen op het Internet die een interesse delen. Ze zijn vergelijkbaar met chatrooms, behalve dat de berichten niet verschijnen op het moment dat ze worden geschreven en dat meer mensen er toegang tot hebben.

Online: rechtstreeks via bijvoorbeeld een telefoonlijn in verbinding staan met een andere computer. Dat kan met een provider zijn en daardoor met internet.

Provider: zie aanbieder.

Server: een machine die de zware klussen afhandelt zoals het sorteren en versturen van e-mail, het onderhouden van sites en het aanbieden van websites aan klanten.

SPAM: de internetversie van 'junk e-mail'. 'Spamming' betekent hetzelfde bericht versturen aan een grote hoeveelheid gebruikers. Meestal gaat het om advertenties.

Startpagina (homepage): de internetpagina waarmee de browser begint zodra deze is gestart. 1. de voornaamste pagina van een website, de voordeur. 2. iemands persoonlijke pagina op het Web. 3. de pagina waarmee een web browser opent. 4. Naam van een handige website met gerubriceerde onderwerpen.

Trojan horse: ook wel Trojaans paard: een onschuldig ogend computerprogramma met kwade bedoelingen. Het doet zich voor als een bruikbaar stuk software, maar - eenmaal genesteld in de computer van het slachtoffer – stuurt het vertrouwelijke informatie naar de maker ervan.

Update: verbetering van een softwareprogramma. Een update wordt vaak gebruikt voor de modernisering van een programma.

USB: afkorting van Universal Serial Bus. Nieuwe standaard voor het aansluiten van allerlei zeer uiteenlopende apparatuur.

URL: afkorting van Uniform Resource Locator. Dit is een onderdeel van een Internetadres dat wordt weergegeven in een vorm die voor iedere web browser begrijpelijk is. Het is een standaard soort adres voor ieder bestand, voorwerp of bron op het Internet. Het adres van een website begint met http://.

Upload: bestanden van eigen computer naar een andere computer kopiëren. Dat kan een computerprogramma, tekst, beeld of geluid zijn. Het tegenovergestelde van uploaden is downloaden.

Virus: een computervirus kan informatie op uw computer uitwissen en grote problemen veroorzaken.

Wereld Wijde Web (World Wide Web): het Web is een universele verzameling van webpagina's, die door hyperlinks met elkaar worden verbonden.

Zoekmachine (search engine): een grote gegevensbank van internetadressen. Internetgebruikers kunnen deze op het Web bezoeken om vragen te stellen betreffende hun zoektocht. Bekende zoekmachines zijn Google en Yahoo.