Protocol

Internet en E-mailgebruik

a. Werknemersreglement
b. Leerling-reglement
c. BIJLAGE: Leeswijzer reglementen

Dit reglement is opgesteld op het directeurenoverleg van maandag 7 oktober 2013

Het vervangt hiermee de eerder opgestelde beleidsstukken:

- **Personeelsbeleid elektronisch verkeer (december2008)**
- **Protocol cyberpesten (januari 2010)**
- **Sociaalmedia protocol onderwijs**

De Oorsprong

Deel A Inhoud:

Deel B Inhoud:

De Oorsprong

Deel A: werknemersreglement

1 Reglement ICT- en internetgebruik voor werknemers

Met deze gedragscode wil de school enkele regels stellen voor verantwoord e-mail- en internetgebruik en de manier waarop wij daarop controle en toezicht mogen houden. Onder 'internet' verstaan wij niet alleen e-mail en bezoeken van het World Wide Web, maar ook andere diensten zoals FTP, Usenet, Facebook, LinkedIn en Twitter.
Deze gedragscode is ingevoerd met instemming van de GMR.

2 Uitgangspunten

Deze gedragscode bevat regels ten aanzien van verantwoord computer-, e-mail- en internetgebruik en over de wijze waarop controle op persoonsgegevens van e-mail- en internetgebruik plaatsvindt.
Het gebruik van internet en e-mail is voor (veel van) de werknemers binnen de organisatie noodzakelijk om hun werk goed te kunnen doen. Aan het gebruik hiervan zijn echter risico's verbonden die nopen tot het stellen van gedragsregels. Tegen de achtergrond van deze risico's mag van de werknemers verantwoord gebruik van internet en e-mail worden verwacht.
De organisatie is gerechtigd tot het geven van voorschriften voor gebruik van internet en e-mail en het nemen van maatregelen ter bevordering van de goede orde in de organisatie. Dit reglement is de weerslag daarvan. Het reglement heeft als doel regels te stellen en controle te kunnen uitoefenen ten behoeve van

- begeleiding/individuele beoordeling,
- voorkomen van negatieve publiciteit,
- tegengaan van seksuele intimidatie, discriminatie en andere strafbare feiten.
- bescherming van vertrouwelijke informatie van de organisatie en van leerlingen en ouders,
- systeem en netwerkbeveiliging, en
- kosten- en capaciteitsbeheersing.

De controle op gebruik van e-mail- en internetgebruik is een verwerking van persoonsgegevens in de zin van de Wet bescherming persoonsgegevens en daarom onderworpen aan de regels en beperkingen daaruit. De organisatie zal dan ook de controle en handhaving van deze regels conform de wet en het algemene arbeidsrechtelijk kader uitvoeren. Gestreefd wordt daarom naar een goede balans tussen verantwoord computer-, e-mail- en internetgebruik en bescherming van de privacy van werknemers op de werkplek.
Gegevens worden alleen verzameld en gebruikt voor deze doelen. Daarbij zal het bestuur te allen tijde de Wet Bescherming Persoonsgegevens en andere relevante wet- en regelgeving naleven. In het bijzonder zal het bestuur de bij controle vastgelegde gegevens beveiligen tegen ongeautoriseerde toegang en mensen met toegang daartoe contractueel verplichten tot afdoende geheimhouding.

3 Computergebruik

Computer- en netwerkfaciliteiten worden aan de werknemer voor gebruik in het kader van zijn functie beschikbaar gesteld. Gebruik is daarom verbonden aan taken die voortvloeien uit deze functie.
Onder dergelijk gebruik valt vooral:

- Voorbereiden schoolwerk en evalueren groepswerk;
- Invoeren rapportgegevens en leerling verslagen;
- Opzoeken van relevante informatie t.b.v. het onderwijs;
- Opzoeken, uitvoeren en beheren lesmateriaal.

Onder lestijd worden computer- en netwerkfaciliteiten alleen gebruikt voor direct met het onderwijs verband houdende doelen. Overig gebruik, zoals het invoeren van toetsresultaten of het beantwoorden van e-mails, vindt zoveel mogelijk buiten de lestijd plaats. Buiten lestijd is beperkt persoonlijk gebruik van de computer toegestaan.
De werknemer draagt er zorg voor dat privacygevoelige gegevens niet toegankelijk zijn voor onbevoegden.
De organisatie kan voor onderwijs- en aanverwante doeleinden systemen voorschrijven, zoals een Elektronische Leeromgeving, een e-mailsysteem of multimediadiensten. De werknemer zal voor het delen van lesmateriaal alleen deze systemen gebruiken en de daarbij gestelde beperkingen en eisen stipt naleven. Het vertonen van informatie uit openbare bronnen (zoals YouTube) valt hier niet onder.
Het installeren van software op de computer- en netwerkfaciliteiten van de organisatie is niet toegestaan zonder toestemming van het systeembeheer. Evenzo is het aansluiten van eigen randapparatuur (zoals laptops, tablets en telefoons) niet toegestaan zonder aparte toestemming daarvoor. Het systeembeheer kan aan de toestemming regels verbinden, zoals het moeten installeren van virusscanners.
De gebruikers van de leeromgeving dienen te allen tijde zorgvuldig om te gaan met de inloggegevens. Wachtwoorden worden niet gedeeld, ook niet incidenteel. Bij een vermoeden van misbruik van een wachtwoord kan de systeembeheerder per direct het getroffen account ontoegankelijk maken.
Het opslaan van privébestanden of -informatie op systemen van de organisatie is toegestaan, mits dit niet storend is voor de dagelijkse werkzaamheden en het netwerk. De organisatie is echter niet verplicht hiervan reservekopieën te maken of kopieën beschikbaar te stellen bij vervanging of reparatie van de betreffende systemen.

4 Vervaardiging en gebruik van beeldmateriaal

De werknemer respecteert de privacy van de leerlingen en is terughoudend in het vervaardigen en gebruiken van beeldmateriaal van leerlingen. Bij het maken van beeldmateriaal worden geen individuele leerlingen getoond. Geen beeldmateriaal wordt gemaakt in privacygevoelige situaties.
Het met toestemming gebruik van beeldmateriaal zal worden beperkt tot publicatie op een

website, weblog of sociale mediasite (zoals Hyves of Facebook) die gekoppeld is aan de organisatie, en daarbij alleen in afgeschermde vorm zodat alleen werknemers, leerlingen en ouders daar toegang toe hebben. Publicaties in andere vormen of in openbare media vereist aparte toestemming van het bestuur. Uitzondering is publicatie van klassenfoto's en sfeerfoto's op de schoolwebsite. Nadrukkelijk niet toegestaan is publicatie op een privéwebsite of privé sociale mediaprofiel van de werknemer.
Dit artikel geldt ook indien gebruik wordt gemaakt van camera's, mobiele telefoons en andere opnameapparatuur die privé-eigendom is. De organisatie kan bij een vermoeden van overtreding verlangen dat werknemer inzage geeft in de betreffende opnames of publicaties daarvan.

5 Gebruik van e-mail

Het e-mailsysteem en de bijbehorende mailbox en e-mailadres wordt aan de werknemer voor gebruik in het kader van zijn functie beschikbaar gesteld. Gebruik is daarom verbonden aan taken die voortvloeien uit deze functie.
Beperkt persoonlijk gebruik van het e-mailsysteem is echter toegestaan, mits dit niet storend is voor de dagelijkse werkzaamheden. Verboden is echter:

- het verzenden van berichten met een pornografische, racistische, discriminerende, beledigende of aanstootgevende inhoud;
- het verzenden van berichten met een (seksueel) intimiderende inhoud;
- het verzenden van berichten die (kunnen) aanzetten tot discriminatie, haat en/of geweld;
- berichten te versturen aan grote aantallen ontvangers tegelijk, kettingbrieven te versturen of bewust virussen, Trojaanse paarden, spyware en dergelijke te versturen.

De werknemer gebruikt bij voorkeur voor privémail een externe webmaildienst (zoals Gmail of Hotmail). De organisatie zal dergelijke diensten niet blokkeren of monitoren, behalve voor controle op bedrijfsgeheimen of op handhaving van het hierboven genoemde verboden gebruik tegenover collega's of relaties van de organisatie.
In het algemeen geldt: probeer zoveel mogelijk op een email van ouders te reageren via de telefoon of door een persoonlijk gesprek. (email is vaak voor meerdere uitleg vatbaar)

6 Internetgebruik

De toegang tot internet en bijbehorende faciliteiten worden aan de werknemer voor gebruik in het kader van zijn functie beschikbaar gesteld. Gebruik is daarom verbonden aan taken die voortvloeien uit deze functie. Beperkt persoonlijk gebruik van het internet is echter toegestaan, mits dit niet storend is voor de dagelijkse werkzaamheden en dit geen verboden gebruik oplevert zoals hieronder aangegeven.
Het is de werknemer niet toegestaan om op internet sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten. Noch is het toegestaan dergelijk materiaal te downloaden

Het is de werknemer niet toegestaan om filesharing- of streamingdiensten (zoals internetradio of Uitzending gemist) te gebruiken wanneer dit overmatig veel dataverkeer genereert. Eveneens niet toegestaan is films, muziek, software en overig auteursrechtelijk beschermd materiaal te downloaden van een evident illegale bron.
Het is de werknemer niet toegestaan om onder lestijd internettoegang te gebruiken voor privédoeleinden. Hieronder valt onder meer het gebruikmaken van sociale netwerken (zoals YouTube, Hyves of Facebook) of chatprogramma's, tenzij dit noodzakelijk is voor het verzorgen van de les.

7 Bijzondere bepalingen voor systeembeheerders

Omdat systeembeheerders in beginsel alle informatie en handelingen van werknemers van de organisatie kunnen inzien, hebben zij een bijzondere positie. Systeembeheerders dienen privacygevoelige informatie en persoonsgegevens die zij in het kader van hun activiteiten als systeembeheerder te weten komen, strikt vertrouwelijk te behandelen. Schending van deze plicht wordt gezien als een ernstig plichtsverzuim, gezien hun bijzondere positie.
Systeembeheerders streven bij hun activiteiten naar maatregelen die inzage in privacygevoelige informatie of persoonsgegevens van individuele werknemers zo veel mogelijk beperken. Zij zullen waar mogelijk slechts geautomatiseerd controleren of filteren zonder daarbij zichzelf of andere personen inzage te geven in gedrag van individuele personen.
Systeembeheerders verschaffen zich slechts toegang tot accounts of computers van werknemers als daar een duidelijke aanleiding toe is of de werknemer daarvoor zijn toestemming heeft gegeven. Toegang zonder deze toestemming is slechts toegestaan in dringende gevallen of bij een duidelijk vermoeden van schending van deze gedragscode. De werknemer zal in dat geval achteraf worden geïnformeerd.
Het bestuur zal systeembeheerders geen opdrachten of dienstbevelen geven ten aanzien van privacygevoelige informatie en persoonsgegevens die in strijd zijn met deze gedragscode.

8 Gebruik van sociale media

De organisatie ondersteunt de open dialoog en de uitwisseling van ideeën en het delen van kennis van de werknemer met vakgenoten via sociale media (zoals Hyves, Facebook, YouTube, Skype, Omegle, Twitter of LinkedIn). Indien dit werkgerelateerde onderwerpen betreft, dient de werknemer ervoor te zorgen dat het profiel en de inhoud in overeenstemming is met hoe hij zich in tekst, beeld en geluid zou presenteren ten overstaan van collega's, ouders en leerlingen.
De werknemer zal terughoudend zijn bij het gebruik van sociale media voor zaken die raken aan zijn functioneren of positie als werknemer voor de school. Wanneer gebruik het delen van kennis met vakgenoten betreft, zal werknemer in beginsel alleen zijn

functie en naam vermelden. Indien het vermelden van de naam van de organisatie wenselijk is, zal de werknemer daarbij vermelden op persoonlijke titel te spreken.
Werknemer zal geen leerlingen toevoegen als ‘vrienden’ of contacten op dergelijke sociale media, tenzij hij hiertoe een apart profiel hanteert dat duidelijk aan de organisatie gelinkt is en waar de organisatie eisen ten aanzien van presentatie, inhoud en functioneren aan kan stellen. Bij beëindiging van het dienstverband zullen werknemer en werkgever een passende oplossing zoeken voor het overdragen van dit profiel of de informatie en contacten daarop.
Bestuurders, managers, leidinggevenden en anderen die namens de organisatie beleid of strategie uitdragen hebben een bijzondere verantwoordelijkheid bij het gebruik van sociale media, ook als de inhoud niet direct verband houdt met hun werk. Op grond van hun positie moeten zij nagaan of zij op persoonlijke titel kunnen publiceren. Zij zijn zich ervan bewust dat medewerkers lezen wat zij schrijven.
Dit artikel geldt ook indien werknemers vanaf privécomputers of -internetaansluitingen deelnemen aan sociale media, doch uitsluitend voor zover het gaat om deelname die het werk kan raken.

9 Voorwaarden voor controle

Controle van persoonsgegevens over e-mail- en internetgebruik vindt slechts plaats in het kader van handhaving van de regels uit dit reglement. Verboden e-mail- en internetgebruik wordt zo veel mogelijk softwarematig onmogelijk gemaakt. Controle beperkt zich in beginsel tot verkeersgegevens van het e-mail- en internetgebruik. Slechts bij zwaarwegende redenen vindt controle op de inhoud plaats.
Controle vindt in beginsel plaats op het niveau van geanonimiseerde gegevens die niet herleidbaar zijn tot identificeerbare personen.
Het systeembeheer/de systeembeheerder is aan geheimhouding gebonden als men om technische redenen kennis moet nemen van persoonsgebonden informatie. Bevindingen worden alleen met de directie gedeeld als daar een concrete, zwaarwegende reden voor is.
In geval van ziekte of langdurige afwezigheid van een werknemer is het bestuur gerechtigd een vervanger of leidinggevende toegang tot de bestanden of mailbox van de werknemer te verschaffen. Deze mag zich echter geen toegang verschaffen tot als privé gemarkeerde mappen of als privé herkenbare mails. Indien de werknemer geen dergelijke markeringen heeft, kan het bestuur door inschakeling van een vertrouwenspersoon de betreffende informatie van de werknemer controleren om zo privé-informatie te herkennen en apart te plaatsen alvorens de vervanger of leidinggevende toegang krijgt.
Indien een werknemer of een groep werknemers wordt verdacht van het overtreden van regels, kan gedurende een vastgestelde (korte) periode gerichte controle plaatsvinden. Voorafgaand aan het starten van deze periode zal het bestuur de vermoedelijke overtreding, de groep en de wijze van controleren documenteren en aanmelden bij de GMR.
E-mailberichten van leden van de GMR onderling, van bedrijfsartsen en van een ieder die zich op grond van zijn functie op enige vertrouwelijkheid moet kunnen beroepen, worden niet gecontroleerd. Dit geldt niet voor geautomatiseerde controle op de veiligheid van het e-mailverkeer en netwerk.

10 Rechten van de werknemer

Het bestuur informeert de werknemer voorafgaand aan de controle op persoonsgegevens over e-mail en internetgebruik, over de doeleinden, de aard van de gegevens, de omstandigheden waaronder zij verkregen zijn en de inhoud van deze regeling.
De werknemer kan zich tot het bestuur wenden met het verzoek voor een volledig overzicht van zijn bewerkte persoonsgegevens. Het verzoek wordt binnen 4 weken beantwoord.
De werknemer kan het bestuur verzoeken zijn persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen indien deze feitelijk onjuist zijn, voor het doel onvolledig of niet ter zake dienend zijn, dan wel in strijd met een wettelijk voorschrift zijn. Het verzoek wordt binnen 4 weken beantwoord.
De werknemer kan verder verzet aantekenen tegen de verwerking van zijn persoonsgegevens in verband met zwaarwegende persoonlijke omstandigheden. Het bestuur oordeelt binnen vier weken na ontvangst van het verzet of dit gerechtvaardigd is. Indien het bestuur het verzet gerechtvaardigd acht, beëindigt zij terstond de verwerking.

11 Sancties

Bij handelen in strijd met deze gedragscode of de algemeen geldende wettelijke regels, kan het bestuur afhankelijk van de aard en de ernst van de overtreding disciplinaire maatregelen treffen. Hieronder vallen een waarschuwing, berisping, overplaatsing, schorsing en beëindiging van de arbeidsovereenkomst.
Werknemers ten aanzien van wie geconstateerd is dat zij zich niet aan deze gedragscode houden, worden zo spoedig mogelijk door de leidinggevende op hun gedrag aangesproken. Zij krijgen daarbij inzage in de over hen vastgelegde gegevens en hebben de gelegenheid te reageren op het geconstateerde. Werknemer en leidinggevende maken dan afspraken voor de toekomst en bepalen de mogelijke sanctie(s) bij overtreding daarvan. Deze afspraken kunnen strenger zijn dan het in deze gedragscode bepaalde. Ook kan de toegang tot e-mail of internet worden beperkt of geheel worden afgesloten.
Disciplinaire maatregelen (behalve een waarschuwing) kunnen niet enkel op basis van een langs geautomatiseerde uitgevoerde verwerking van persoonsgegevens worden getroffen, zoals een constatering van een automatisch filter of blokkade. Voorts worden geen disciplinaire maatregelen getroffen zonder dat de werknemer gelegenheid heeft gekregen zijn zienswijze naar voren te brengen.

12 Slotbepaling

Deze regeling wordt jaarlijks geëvalueerd door het bestuur en de GMR. De eerstkomende evaluatie vindt plaats in oktober 2014.
De organisatie kan deze gedragscode met instemming van de GMR wijzigen als de omstandigheden daar aanleiding toe geven. Voorgenomen wijzigingen worden voorafgaand aan de invoering aan de werknemers bekend gemaakt. Het bestuur zal feedback van werknemers in overweging nemen alvorens de wijzigingen in te voeren.

Deel B: leerling-reglement

gedragscode leerlingen en ouders

Inleiding

De huidige tijd kenmerkt zich door een overvloed aan informatie die op eenvoudige wijze bereikbaar is. Sinds de school informatiekanalen als televisie (en video) en meer recent, internetfaciliteiten ter beschikking heeft, kunnen er beelden en programma's de school binnenkomen en uitgaan, die ongeschikt zijn voor leerlingen. Denk aan bepaalde uitingen van geweld, seks en racisme. Met name door de gemakkelijke toegang tot internet, wordt het risico op het binnenhalen van onfatsoenlijk, disrespectvol en ongewenst materiaal steeds groter. Leerlingen moeten leren daar mee om te gaan.
Als school willen wij leerlingen leren hoe hiermee om te gaan. Wat is goed en wat niet, wat kan en wat niet. We benaderen het gebruik van het internet/e-mail, zoals we ook kinderen leren omgaan met het verkeer of de televisie. Indien er zich een bepaalde situatie voordoet, wordt daar op ingespeeld.
De gedragscode uit dit document legt vast hoe wij als school willen omgaan met gewenst en ongewenst gedrag op het gebied van gebruik van internetfaciliteiten en computers.

1 Algemene aanpak

Het is ons doel dat leerlingen ‘mediawijs’ van school gaan: in de hoogste groepen wordt jaarlijks aandacht besteed aan ontwikkelingen op het gebied van moderne communicatie en eventuele risico’s. In eerst instantie doen zij dit onder begeleiding/toezicht van de leerkracht en beperkte keuze mogelijkheid. Naarmate leerlingen meer ervaring opdoen met internet en computers krijgen zij meer vrijheid, maar natuurlijk blijven leerlingen onder schooltijd de verantwoordelijkheid van de school.
Wij stellen dan ook regels over toegang tot media en internet, en over het gebruik ervan. Zo stelt de school kinderen niet bewust bloot aan beelden van geweld, seks en racisme, die geen opvoedkundige bedoeling hebben. Een uitzondering hierop is bijvoorbeeld: het school-tv-weekjournaal voor groep 7 en 8, hierin kunnen nieuwsonderwerpen behandeld worden, die oorlogssituaties en dergelijke betreffen. Ook volgen wij de Kijkwijzer bij het vertonen van films. En waar het internet en e-mail betreft, willen wij voorkomen dat er onprettige zaken gebeuren (zoals pesten per e-mail) of leerlingen met ongewenste informatie of gebeurtenissen te maken krijgen.

Internet en e-mail stellen wij beschikbaar voor schoolzaken, zoals het gezamenlijk maken van werkstukken. Leerlingen mailen dan ook op school alleen over onderwerpen die met school te maken hebben. De leerlingen mogen gebruik maken van het schoolmail- adres voor privézaken. Voor schoolzaken kunnen zij gebruik maken van hun privé e-mailadres.

De regels over internet en e-mailgebruik zijn erop gericht om bovenstaande te realiseren. Een totaal verbod op het privégebruik van elektronische informatie- en communicatie-middelen zoals het versturen en ontvangen van persoonlijke e-mailberichten is niet reëel. De school stelt wel beperkende voorwaarden aan het privégebruik.

2 Afspraken met leerlingen

De onderstaande afspraken geven weer hoe ons algemeen beleid zich vertaalt in concrete regels voor leerlingen.
Deze afspraken worden als los document aan de leerling aangeboden, die dit moet tekenen voordat hij gebruik mag maken van computers en of internet. Een kopie van deze afspraken wordt goed zichtbaar opgehangen bij de computerfaciliteiten.

2.1 Algemene afspraken

- Ik gebruik internet in hoofdzaak voor zaken die verband houden met mijn leeractiviteiten. Tijdens de les ga ik niet op websites die niets met de les of school te maken hebben. Ook gebruik ik geen andere programma's (zoals Hyves) die niets met de les of school te maken hebben
- Ik ga direct naar de meester of juf als ik op internet vervelende informatie tegenkom en/of geblokt ben.
- Ik download geen software en kopieer of wijzig geen materiaal dat voorzien is van copyright; bij twijfel over rechten vraag ik eerst toestemming van de leerkracht.
- Ik vertel geen wachtwoorden van mezelf of anderen zonder toestemming door.
- Ik maak in school geen kwetsende of beledigende opmerkingen, voorstellingen of materialen, en plaats deze ook niet op internet.
- Ik reageer niet op gemene, valse of vervelende berichten. Het is niet mijn schuld dat sommige mensen zich niet weten te gedragen. Als ik zulke berichten krijg waarschuw ik meteen mijn juf, meester of ouders, zodat die op hun beurt de ICT-coördinator kunnen verzoeken hiertegen maatregelen te nemen.
- Ik zal niet opzettelijk het netwerk of werk van anderen op de computer beschadigen.
- Ik geloof niet alles wat ik op het internet zie of lees.

2.2 Afspraken over privacy

- Ik zal alleen mijn voornaam gebruiken op internet. Ik geef anderen op internet geen persoonlijke gegevens zoals: adressen, telefoonnummers, mijn eigen e-mailadres of het e-mailadres van mijn ouders of andere bekenden. Bij klasgenoten en vriendjes/vriendinnetjes mag dit wel maar dan zal ik ze eerst laten beloven of zij er ook zo netjes mee om zullen gaan.
- Ik zal geen foto's of filmpjes maken van klasgenoten of andere leerlingen op school, of van een meester of juf, of die op internet zetten zonder dat apart te vragen. En als ik ze op internet mag zetten, doe ik dat op een plek waar niet iedereen ze kan zien.
- Als de meester of juf het vraagt, laat ik zien welke foto's of filmpjes ik heb gemaakt van klasgenoten of anderen. Als deze de regel hierboven overtreden, of als ze rare

dingen laten zien, dan moet ik die wissen.
- Ik geef nooit toestemming aan iemand, die ik op het internet ben tegengekomen, om mij in het echt te ontmoeten.
- Ik zal personen die ik op het internet ben tegengekomen, geen foto's van mijzelf toesturen, behalve als mijn ouders, meester of juf hiervoor toestemming hebben gegeven.

2.3 Afspraken over websites

- Ik bezoek niet expres sites die informatie bevatten die niet voor kinderen bedoeld is. Mocht dit per ongeluk toch gebeuren dan sluit ik de site.
- Ik gebruik bij het werken met een zoekmachine normale woorden (zoektermen). Ik gebruik geen woorden die te maken hebben met grof woordgebruik, seks of geweld. Bij twijfel overleg ik met de meester of juf.
- Ik bezoek geen internetsites die niks met school te maken hebben, behalve in de pauze of als de meester of juf apart toestemming hebben gegeven. Ik zal ervoor zorgen dat niemand er last van heeft als ik zo'n site bezoek.

2.4 Afspraken over e-mailen

- Ontvang ik een e-mail van iemand die ik niet ken, dan meld ik dit aan mijn juf of meester.
- Ik mail alleen met mijn eigen account. Als ik zie dat andere mensen hun account onbeheerd laten, dan zal ik dat voor ze afsluiten.
- Ik zal geen kettingbrieven of e-mailberichten met een dreigende inhoud doorsturen, ook niet als ze zeggen bedoeld te zijn als grap.
- Ik antwoord niet op reclamemail, omdat de kans groot is dat ik er nog meer ontvang als ik het wel doe.
- Als ik mail ontvang afkomstig van mensen die ik niet ken of met onderwerptitels die ik niet snap, verwijder ik het bericht en leeg de e-mail prullenbak.
- Ik mag alleen mijn voornaam gebruiken. Ik geef anderen op internet geen persoonlijke gegevens zoals: adres, telefoonnummer, mijn eigen e-mailadres of het adres van mijn ouders of andere bekenden.
- Als de computer merkt dat ik dingen verstuur die niet mogen, dan krijgt de meester of juf daar een melding van.

3 Controle en handhaving

Bij regels hoort ook controle en handhaving. Hierbij dienen wij als school rekening te houden met het recht van het kind op privacy. Dit betekent dat wij onder normale omstandigheden geen kennisnemen van mails of andere bestanden van kinderen die als privé bedoeld zijn. In uitzonderlijke situaties, zoals bij pesterijen of concreet vermoeden van strafbare feiten, heeft de school het recht, om de door de school beschikbaar gestelde mailboxen en op haar systemen opgeslagen bestanden van de leerlingen in te kunnen zien en te kunnen controleren.
De betrokken leerkracht of ICT-coördinator zal daarbij strikte vertrouwelijkheid in acht nemen voor niet-relevante informatie. Informatie zal niet worden gewist zonder toestemming van de ouders. De school zal geen toegang eisen tot privémailboxen van leerlingen, maar kan in de genoemde uitzonderlijke situaties wel eisen dat de leerling informatie (zoals foto's of teksten) verwijdert uit bijvoorbeeld de mobiele telefoon. Denk aan een zonder toestemming gemaakte foto of een aanstootgevende tekst.

4 Monitoren van internet- en e-mailgebruik

De school heeft een filter geïnstalleerd om ongewenst geachte websites en internetdiensten te blokkeren. De school kan met geautomatiseerde processen periodieke controles uitvoeren op ongewenste zoekwoorden betreffende pesten, seks en andere overlastgevende onderwerpen. Dit geldt zowel voor internetgebruik als e-mailgebruik.
De leerkracht heeft de mogelijkheid om via speciale software "mee te kijken" op de computers van leerlingen. Deze software kan tijdens de les worden gebruikt voor educatieve doeleinden. Buiten lestijd zal de leerkracht een computer alleen oproepen via deze software bij een concreet vermoeden van overtreding van dit protocol.
De resultaten van controles of meekijken worden met de leerling besproken. Op verzoek zal de school aan de ouders inzage geven in welke zoekwoorden worden gebruikt, of en hoe de leerkracht het internetgebruik van leerlingen volgt en leest en wat er met de bevindingen gebeurt.

5 Sancties bij overtredingen

5.1 Waarschuwingen

Bij overtreding van de bovenstaande regels krijgt de betrokken leerling één (1) individuele waarschuwing van de groepsleerkracht. Bij overtreding ten aanzien van de regel over mobiele telefoons kan de groepsleerkracht de telefoon innemen voor de rest van de dag. De leerkracht zal de telefoon op een veilige plaats bewaren. De leerkracht zal niet zelf toegang tot opgeslagen informatie zoeken tenzij de leerling of diens ouders daar toestemming voor verlenen.

5.2 Tijdelijke ontzegging

Wanneer blijkt dat er voor een 2e maal binnen het schooljaar een overtreding plaatsvindt, wordt de leerling de toegang tot het internet voor een bepaalde periode ontzegd. De ouders worden hiervan, indien mogelijk dezelfde dag, telefonisch op de hoogte gebracht door de groepsleerkracht. Duur en omvang van de ontzegging zullen door de groepsleerkracht worden vastgesteld op basis van de aard van de overtreding. Bij een overtreding van de regels over beeldgebruik begaan met de mobiele telefoon, kan de groepsleerkracht de telefoon in beslag nemen en eisen dat het kind of de ouders de betreffende beelden wissen. De leerkracht zal niet zelfstandig beelden wissen.

5.3 Langdurige ontzegging

Bij een 3e overtreding kan de leerling de toegang tot het internet voor langere tijd (zelfs voor de rest van het schooljaar) worden ontzegd. Duur en omvang van de ontzegging zullen door de directie worden vastgesteld op basis van de aard van de overtreding. Ook in dit geval worden de ouders hiervan, indien mogelijk dezelfde dag, telefonisch door de groepsleerkracht op de hoogte gebracht. Tevens worden de ouders schriftelijk, middels een brief van de directie, van dit besluit op de hoogte gesteld.

5.4 Ernstige overtredingen

Als de leerling een bericht plaatst op internet of per e-mail verstuurt dat in ernstige mate ontoelaatbaar is (opruiend, hatelijk, onsmakelijk etc.), of de wet overtreedt (bijvoorbeeld door valse beschuldigingen te doen), zal de groepsleerkracht direct contact opnemen met de ouders.
Bij een vermoeden van strafbare feiten kan de directie besluiten contact op te nemen met bureau HALT of de politie. De betreffende informatie wordt afgedrukt, en wordt samen evenals de digitale kopie bewaard, als potentieel bewijsmateriaal. De ouders krijgen een kopie van dit materiaal en worden tijdig geïnformeerd over de stappen die de school van plan is te nemen. Daarbij zal de school de reactie van de ouders meewegen.
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. De school zal hiermee rekening houden en geen sancties opleggen als niet afdoende vaststaat dat de betrokken leerling daadwerkelijk de afzender is.

BIJLAGE

Inhoud:

1 Toelichting op de modelreglementen

Het monitoren en reguleren van internet- en e-mailgebruik is een juridisch lastige kwestie. Hoewel gebruik van deze middelen steeds populairder wordt, en de behoefte aan reguleren en controleren daarmee groter, stelt de wet strenge eisen. In deze toelichting op de door ons opgestelde reglementen beschrijven wij de juridische achtergrond, de beperkingen en regels uit de wet en de keuzes die zijn gemaakt.
Dit advies begint met een algemene achtergrond over privacy op het werk. Daarna bespreken wij enkele vuistregels die bij ieder beleid op dit punt gesteld moeten worden, alsmede hoe de reglementen ingevoerd moeten worden. Vervolgens worden artikelsgewijs de reglementen besproken voor leerlingen en voor werknemers (leerkrachten).

2 Algemene achtergrond over privacy

Privacy is een grondrecht, dat beschermd wordt door diverse wetten en internationale verdragen. Ook op het werk en ook op school bestaat dus privacy. Werkgevers, leerkrachten en schoolbesturen mogen niet zomaar bijhouden wat mensen doen, ook niet bij privégebruik van internet, e-mail of telefoon. De regels over wat wel en niet mag, en wat de werkgever kan controleren, moeten in een reglement worden vastgelegd.
Bedrijfsmiddelen zoals internettoegang krijgt men omdat ze nodig zijn voor het werk. Ze zijn eigendom van de werkgever, en deze mag dus eisen stellen aan het gebruik ervan. Van de werknemer mag worden verwacht dat hij verantwoordelijk, professioneel en integer omgaat met de bedrijfsmiddelen die hij krijgt. Net zo goed als dat de werkgever regels mag stellen over lunchen in vergaderruimtes, mag hij regels stellen over gebruik van internet. De werkgever heeft natuurlijk geen plicht om werknemers gebruik te laten maken van internet. Maar in veel bedrijven/scholen is toegang tot internet onvermijdelijk om het werk goed te kunnen doen.
Daar staat tegenover dat werknemers een “redelijk niveau” van privacy mogen verwachten. Hetzelfde geldt voor leerlingen. Hiermee ontstaat natuurlijk een spanningsveld: dit beroep op privacy botst met de (terechte) wens van leraren of schoolbesturen om ongewenst gedrag te monitoren of te voorkomen. Dit spanningsveld oplossen is geen eenvoudige kwestie. De wet kent geen harde regel zoals “ter voorkoming van overlast mag alles” of “monitoren mag wanneer men maar dit tijdig meldt” of “de school heeft een zorgplicht dús mag men de leerlingen permanent volgen”. Integendeel, de wet schrijft voor dat steeds een belangenafweging moet worden gemaakt.
Concreet komen deze regels erop neer dat er óf toestemming moet zijn, óf de werkgever (het schoolbestuur) een dringende noodzaak moet hebben die zwaarder weegt dan de privacy van de werknemer, ouder of leerling. Aan dit laatste vereiste is niet snel voldaan.
Het vragen van toestemming lijkt eenvoudig: laat mensen een formuliertje tekenen dat alles mag, en klaar is Kees. Maar dat is voor de wet niet genoeg. De toestemming moet op vrije wil gebaseerd zijn.

Een werkgever kan dus niet zomaar iemand opdragen te tekenen, en al helemaal niet dreigen het contract niet te verlengen als er niet wordt getekend voor de toestemming.
Voor leerlingen en hun ouders geldt dat in beginsel wél bij inschrijving bij het nieuwe schooljaar, maar niet tijdens het jaar, toestemming kan worden gevraagd. De toestemming tot de verwerking is daarmee een voorwaarde voor inschrijving geworden. Maar halverwege het jaar 'zomaar' toestemming vragen, is problematisch omdat de ouders dit moeten mogen weigeren en de school zal dit moeten respecteren.
Overigens geldt daarbij nog dat leerlingen die geen zestien zijn, niet zelf toestemming kunnen geven voor welke verwerking van hun persoonsgegevens dan ook. De ouders moeten expliciet deze toestemming geven.

2.1 Vuistregels voor werken met persoonsgegevens

Werken met persoonsgegevens brengt dus juridische risico's met zich mee. Het is niet toegestaan persoonsgegevens te gebruiken als dat niet noodzakelijk is. Om deze risico's te beheersen, bevelen wij de volgende vuistregels aan:

- Gebruik van geanonimiseerde informatie heeft de voorkeur boven informatie waarin personen te herkennen zijn.
- Geautomatiseerde processen hebben de voorkeur boven rapporteren aan leidinggevenden of andere mensen.
- Informatie over herkenbare personen mag alleen worden gebruikt indien dit in het reglement is aangegeven, en dan alleen voor het daar genoemde doel.
- Genoemde doelen moeten concreet en duidelijk zijn.
- Gebruik voor andere doelen is niet toegestaan, tenzij deze in duidelijk verband met elkaar staan.

De eerste vuistregel is meteen de belangrijkste. Maar al te vaak wordt monitoren en rapporteren gebruikt, omdat gegevens nu eenmaal beschikbaar zijn en het dan logisch lijkt deze te verstrekken aan de leidinggevende zodat deze "maatregelen kan nemen". Echter, het is zeker niet gezegd dat dit de beste keuze is.
Stel men streeft naar kosten- en capaciteitsbeheersing bij gebruik van het netwerk. Kosten en capaciteitsproblemen ontstaan door grootschalig internetgebruik, bv. de hele dag internetradio beluisteren. Men kan dan kiezen voor een maatregel waarbij de leidinggevende elke week een mail krijgt met de top 3 veelgebruikers van internet inclusief de populairste webadressen die zij bezoeken.
Men kan echter ook een automatisch mailtje sturen naar deze veelgebruikers om ze te waarschuwen, en pas na herhaalde overtreding de leidinggevende informeren. Ook kan men veelgebruikers 'afknijpen' (hun internetsnelheid terugschroeven) en zo het probleem oplossen. Deze laatste oplossing is meteen een voorbeeld van de tweede vuistregel: met een geautomatiseerde oplossing wordt zo het probleem aangepakt.

2.2 Rechten van de betrokkenen

Daarnaast hebben de betrokken personen de volgende rechten:

- Recht van informatie: Zij moeten kunnen nalezen welke informatie wordt verzameld, op welke wijze dat gebeurt en met welk doel.
- Recht van inzage: Zij mogen een kopie opvragen van de informatie die specifiek voor hen is verzameld.
- Recht van correctie: Zij mogen verlangen dat onjuiste of achterhaalde informatie wordt aangepast.
- Recht van verwijdering: Zij mogen verlangen dat verouderde en irrelevante informatie wordt verwijderd.

2.3 Instemmingsrecht OR en/of (G)MR

Bij grotere organisaties gelden naast de Wet Bescherming Persoonsgegevens ook nog andere wetten wanneer het gaat om verzamelen van persoonsgegevens van werknemers of leerlingen. Deze bepalen vooral welke procedure het bestuur moet voeren wanneer zij beleid wil invoeren waarmee persoonsgegevens worden verzameld.
Wanneer een organisatie een ondernemingsraad heeft, heeft deze instemmingsrecht op alle verwerkingen van persoonsgegevens van werknemers (art. 27 lid 1 sub k Wet op de Ondernemingsraad). Het bestuur is verplicht het conceptreglement aan de OR voor te leggen alvorens het in te voeren. De OR moet er dan minstens één keer over vergaderen en dient dan een beslissing te nemen. Het bestuur mag het reglement niet invoeren (en dus de verwerking niet uitvoeren!) totdat de OR besloten heeft.
Op scholen bepaalt de Wet Medezeggenschap op Scholen (art. 13 sub i) de voorafgaande instemming nodig is van de medezeggenschapsraad. Wanneer het gaat om persoonsgegevens van ouders en leerlingen, moeten specifiek de ouders (en eventuele leerlingen in de GMR) de instemming geven.

3 Toelichting op modelreglement werknemers

Het modelreglement werknemers is geschreven voor scholen die ten aanzien hun leerkrachten (de werknemers) regels willen stellen over internet- en e-mailgebruik. Hier gelden naast de normale regels zoals bij elk bedrijf nog enkele extra regels die specifiek toezien op de relatie leerkracht/leerling. Zo is er de vraag of een leerkracht op zijn eigen Hyves- of Facebookpagina leerlingen mag toevoegen en daar contact mee onderhouden.
De regels uit dit reglement zijn gebaseerd op een algemene belangenafweging voor beide partijen. Waar mogelijk zijn rechten of beperkingen voor beide partijen opgenomen. Een leraar mag bijvoorbeeld enig privégebruik van internet maken op school, maar de school mag wel filteren op ongewenst taalgebruik en mails weren die niet door het filter heenkomen.

3.1 Uitgangspunten

De sectie met uitgangspunten bij het reglement is een belangrijk instrument, omdat deze de

context en achtergrond schetst van het monitoren en de regels die worden opgelegd.
De inleiding is dus geen vrijblijvend verhaal maar een kader waarbinnen alle regels gesteld gaan worden.
Belangrijk is in ieder geval dat in de inleiding de doelen worden genoemd waarvoor de controle met persoonsgegevens plaatsvindt. Genoemd in het modelreglement zijn:

- systeem- en netwerkbeveiliging;
- tegengaan overlastgevend gebruik.

Het gebruik van specifieke doelen is belangrijk. Soms worden zeer generieke termen als 'ongewenst gebruik' gehanteerd. Dit is juridisch niet mogelijk. Doelen moeten concreet en specifiek zijn. Wat 'ongewenst' is, is niet op voorhand te zeggen. Het is dus af te raden daarmee te werken: dergelijke doelen kunnen het reglement mogelijk onderuit halen omdat ze onvoldoende basis bieden.
Andere denkbare doelen zijn:

- bescherming van vertrouwelijke informatie;
- het beschermen van de reputatie van de instelling naar buiten toe;
- kosten- en capaciteitsbeheersing.

Uiteraard moet bij elk doel de rest van het reglement worden aangepast zodat de genomen maatregelen toegelicht worden. Ook moet daarbij de afweging zijn gemaakt dat daarbij de verwerking van persoonsgegevens noodzakelijk is.

3.2 Computergebruik

De sectie computergebruik stelt algemene regels over wat leerkrachten wel en niet mogen doen met de door de school beschikbaar gestelde ICT-faciliteiten. Daarbij is onderscheid gemaakt tussen "tijdens de les" en "buiten de les". In het laatste geval mag er iets meer. Zo mag men bijvoorbeeld tegen het eind van de middag gerust een mailtje naar de partner sturen dat het laat wordt. Maar chatten met de partner tijdens de les is niet toegestaan.
In deze sectie staat een artikel over door de school voorgeschreven systemen zoals een ELO. Als de school een dergelijk systeem hanteert, dient de leerkracht dit ook te gebruiken. Is er bijvoorbeeld voorzien in een systeem voor uploaden en verspreiden van educatieve video's, dan mag de leerkracht niet zelf dergelijke video's uploaden naar YouTube omdat hij dat een prettiger systeem vindt. (Natuurlijk mag hij wel bestaande YouTube-video's vertonen als bronmateriaal in een les.)

3.3 Vervaardiging en gebruik van beeldmateriaal

Het vervaardigen van foto's en video's van leerlingen is een gevoelig punt op veel scholen. Wanneer dit niet goed geregeld is, kan de reputatieschade voor leerkracht én school enorm zijn. Het is daarom belangrijk hier duidelijke regels te stellen – zowel aan leerkrachten als aan leerlingen en ouders. De drie modelreglementen zijn hier onderling op afgestemd.
Van de leerkracht wordt terughoudendheid verwacht bij het maken van beeldmateriaal. Het gekozen uitgangspunt is algemene foto's, zoals sfeerbeeld, en liever geen foto's van individuele leerlingen.

Publicatie van foto's dient op afgeschermde locaties zoals Hyvesprofielen te gebeuren en niet op het openbare internet. Daarbij is gekozen voor de regel dat het profiel verbonden moet zijn aan de school, zodat de school controle kan uitoefenen en (al dan niet op verzoek van ouders) beeldmateriaal kan laten verwijderen.
Als een leerling of ouder beeldmateriaal maakt, kan de leerkracht deze daarop aanspreken op grond van het reglement beeldgebruik, waarover hieronder meer.

3.4 Gebruik van e-mail

De algemene regels van computergebruik zijn hier vertaald naar specifieke regels voor e-mail. Enig privégebruik van de schoolmail is toegestaan (dit is een wettelijk recht dat de school niet mag inperken). De school mag wel filteren. Het verdient aanbeveling dat leerkrachten privé een mailsysteem zoals Gmail of Hotmail gebruiken en niet de schoolmail.

3.5 Internetgebruik

De algemene regels van computergebruik zijn hier vertaald naar specifieke regels voor internet. De algemene doelen zijn hier vertaald naar internetspecifieke regels, zoals het niet mogen gebruiken van "datavreters" zoals internetradio als dat tot hoge kosten leidt. Ook is een verbod opgenomen tot het gebruiken van 'Facebook'en of YouTube tijdens de les.

3.6 Bijzondere bepalingen voor systeembeheerders

De systeembeheerder (die al of niet docent kan zijn) heeft een bijzondere positie: hij kan overal bij. Daarmee zijn extra strenge regels nodig om misbruik van deze positie te voorkomen.

3.7 Gebruik van sociale media

Steeds meer leerkrachten gebruiken sociale media om bij te blijven, te communiceren met collega's uit het vak, en ook om contact met leerlingen of ouders te onderhouden. Omdat hierbij de link met de school snel is gelegd, kan de school hier enige regels aan stellen. Tegelijkertijd kan een school niet zonder meer eisen dat men zich onthoudt van het gebruik van sociale media.
Als uitgangspunt is het delen van vakkennis en discussiëren met vakgenoten genomen, zoals bijvoorbeeld bij het Onderwijs 2.0 initiatief gebeurt. Daar kan een leraar zonder meer aan deelnemen, zolang hij maar uitkijkt geen persoonlijke informatie over leerlingen of negatieve informatie over de school in herkenbare vorm te delen.
Voor contact tussen leraren en leerlingen is terughoudendheid aan te bevelen. Daarom is gekozen voor een regel waarbij de leraar een apart profiel kan aanmaken dat duidelijk aan zijn functie en de school is gekoppeld – kort gezegd "meesterjan.hyves.nl". Daar kan meester Jan contact onderhouden, huiswerkvragen beantwoorden en chatten met leerlingen. Zijn privépagina dient echter dan géén leerlingen als vrienden of contacten te bevatten.

4 Voorwaarden voor controle

Zoals bij de algemene inleiding is besproken, kan een school niet zonder meer elk gebruik op elk moment monitoren op ongedefinieerd “ongewenst gedrag”. De leerkracht heeft een zekere privacy op school. De in dit artikel genoemde aanpak balanceert de privacy en de wens tot controle, uitgewerkt volgens de vuistregels hierboven.
Andere vormen van controle zijn natuurlijk in principe ook mogelijk, mits deze maar voldoen aan de gegeven vuistregels.

4.1 Rechten van de werknemer

Op grond van de WBP heeft de werknemer bepaalde rechten. Deze zijn hier uitgewerkt. Deze clausules zijn dus in feite een vertaling van de wet, die dwingend is. Hiervan afwijken is in beginsel niet mogelijk.

4.2 Sancties

Bij overtreding van de regels uit het reglement kan de school als werkgever sancties opleggen. De genoemde sancties zijn generiek beschreven; de school dient hierin een beslissing te nemen. Aanbeveling verdient wel om de tweede clausule te behouden: bij een eerste overtreding méér doen dan een waarschuwing is moeilijk, behoudens uitzonderingsgevallen.
De derde clausule is een directe vertaling van de WBP: het is wettelijk verboden enkel en alleen op basis van een geautomatiseerde controle een sanctie op te leggen. De resultaten van zo’n controle moeten altijd door een persoon worden beoordeeld alvorens tot een sanctie kan worden besloten. Concreet betekent dit dat bijvoorbeeld wanneer een filter meldt dat ongewenste inhoud wordt verzonden, de leerkracht niet meteen afgesloten mag worden van internet of e-mail. Eerst moet een systeembeheerder of leidinggevende controleren of de inhoud inderdaad in strijd is met het reglement.

4.3 Slotbepaling

De slotbepaling bevestigt wanneer het reglement in werking treedt en dat de GMR dient te worden gehoord.

5 Toelichting bij modelreglement leerlingen

Het modelreglement voor ICT-gebruik door leerlingen dient twee doelen: de school wil hier zowel regels stellen aan ongewenst gedrag, als bijdragen aan het mediawijs worden van de leerlingen. Dit is ook expliciet zo uitgewerkt. Natuurlijk is dat laatste alleen mogelijk als daar ook concreet aandacht voor gegeven wordt in de les. Het is weinig educatief om dit reglement uit te printen en aan de muur te hangen in het computerlokaal.

5.1 Inleiding en algemene aanpak

De uitgangspunten zijn bedoeld als inleiding en om een kader te schetsen. Hiermee worden de uitgangspunten duidelijk gekoppeld aan het algemene beleid of de visie van de school.

5.2 Afspraken met leerlingen

Dit artikel is opgezet als een serie bullets in kindertaal, zodat de leerlingen weten waar ze aan toe zijn. Sommige bullets zijn echte regels, andere zijn alleen maar verstandige tips.
Het reglement is gericht op leerlingen van de basisschool. Deze kunnen niet rechtsgeldig een reglement tekenen. De ouders/verzorgers moeten het tekenen. Zonder handtekening van de ouders/verzorgers kan de school de leerling niet houden aan de plichten uit het reglement.
De bullets uit dit artikel kunnen worden ge-copy-paste naar een apart document dat de leerling moet lezen en tekenen. Dit kan in een ceremoniële gebeurtenis worden uitgevoerd, zodat de leerling wordt doordrongen van het belang van deze regels. Echter, de handtekening van de ouders onder het gehele reglement blijft vereist.
Omdat in het reglement ook wordt voorzien in monitoren en lezen van privécommunicatie dient de toestemming van de ouders uit vrije wil gegeven te worden. Ouders moeten tijd genoeg hebben om het te lezen en eventueel een reactie te geven.

5.3 Controle en handhaving

Zoals bij het modelreglement voor leerkrachten al is besproken, is ongelimiteerd monitoren en volgen van mensen niet toegestaan. Dit geldt ook voor leerlingen. Ook zij hebben privacy. Dit blijkt expliciet uit het Verdrag voor de Rechten van het Kind.
Dit artikel is sterk vergelijkbaar met hoe de werknemer (leerkracht) gecontroleerd mag worden. Het vervolgartikel (Monitoren van internet- en e-mailgebruik) bevat wel een extra clausule over “meekijken”, wat tijdens de les in beginsel gewoon toegestaan is.
De regels voor monitoren en controle zijn bij internet- en ICT-gebruik hetzelfde als bij bijvoorbeeld het doorzoeken van jassen of tassen. Dit mag alleen bij concrete vermoedens van strafbare feiten. Ook moeten de ouders worden ingelicht dat dit kan gebeuren en wanneer. Gebeurt het zonder inlichten vooraf, dan moet er achteraf worden geïnformeerd.

5.4 Sancties

De sancties die worden gesteld zijn gradueel opgebouwd. Er is gekozen voor een streng beleid: na één waarschuwing volgt al een tijdelijke blokkade, en na twee waarschuwingen mag de leerling de rest van het schooljaar in het geheel niet meer internetten.
Hoewel strenge regels nuttig zijn bij de opvoeding, dient een school wel zorgvuldig na te denken of een dergelijk verbod a) handhaafbaar is, b) proportioneel en c) uit te leggen aan de leerling. Vergelijk de regel “wie drie keer een andere leerling omver gooit bij het spelen, mag het hele jaar niet meer rennen op het schoolplein”.
Ontzegging van internet voor een lange periode is een zéér zware sanctie die met de grootst

mogelijke terughoudendheid moet worden gehanteerd. Onder “internetten” valt ook het gebruik van internet bij onderwijs. De leerling mag dan ook geen educatieve spellen meer doen, of op Wikipedia onderzoek doen voor een spreekbeurt.
Voor wat betreft strafbare zaken is een clausule “Ernstige overtredingen” opgenomen. Een complicatie is hier dat basisschoolleerlingen (twaalf-minners) niet strafrechtelijk vervolgd kunnen worden. Hiermee dreigen is dan ook zinloos. Een verwijzing naar Bureau HALT is vaak wel haalbaar. Het is een goed idee op voorhand hierover informatie in te winnen zodat de school weet wat men wel en niet kan toezeggen.

6 Modelreglement beeldgebruik

Zoals hierboven al aangestipt, is het maken en gebruiken van beeld van leerlingen vandaag de dag een gevoelige kwestie.
De regels uit dit reglement proberen zorgvuldig te navigeren in deze. Veel keuzes zijn echter arbitrair, zoals het maximumformaat van foto’s of het verbod op fotograferen door ouders. Andere regels zijn zonder meer denkbaar, zolang daarbij maar het privacybelang van de leerling (ook andere leerlingen dan het eigen kind) in acht wordt genomen.
Dit reglement is in beginsel prima samen te voegen met het modelreglement leerlingen. Echter, dat modelreglement zal gewoonlijk pas worden getekend wanneer de leerling in groep 6 of 7 gebruik gaat maken van de ICT-faciliteiten. De regels over beeldgebruik zijn al eerder wenselijk, vanaf groep 1. Daarom kunnen zij het beste apart als reglement bij de allereerste inschrijving worden gesteld. De ICT-regels kunnen dan later worden toegevoegd.