BOORTMEERBEEK

Policy Informaticamiddelen en veiligheid

A. Algemeen

1. Doel en toepassingsgebied

Het gemeentebestuur stelt aan zijn personeelsleden een aantal communicatiemiddelen ter beschikking in het kader van de uitoefening van hun functie. Het gebruik ervan bevordert zowel de dienstverlening als de werking van het bestuur. Hierbij heeft het gemeentebestuur wettelijke en morele verplichtingen tot het nemen van veiligheidsmaatregelen. Het is dan belangrijk dat personeelsleden een eenduidig verstaanbaar document kunnen raadplegen rond het gebruik van ICT-middelen.

De hierna vastgelegde policy is van toepassing op alle ICT-middelen, IT-infrastructuur en elektronische communicatiemiddelen (o.m. telefoon, GSM, fax, PC, semafoon, modems, e-mail, interne memosystemen, netwerkprogrammatuur, interne en externe netwerken, internet, LAN-, toets- en leerplatformen, administratieve systemen, informatiesystemen, …) en op alle gegevens die door die systemen worden verzonden of erin worden opgeslagen.

De policy is van toepassing op alle categorieën van personeelsleden, stagairs, partners, leveranciers die recht hebben op ICT-middelen van het gemeentebestuur.

2. Verantwoordelijkheden van de gebruiker

De ICT-infrastructuur die aan het personeelslid of elke andere gebruiker ter beschikking is gesteld, blijft eigendom van het bestuur.

De gebruiker draagt als een goede huisvader zorg voor de ICT-infrastructuur die hem ter beschikking is gesteld. Hij gebruikt deze middelen op een professioneel, sociaal, ethisch en juridisch correcte wijze, overeenkomstig de bepalingen in deze policy en de instructies die ter zake worden gegeven.

De gebruiker heeft, voor zover van toepassing, een aantal verantwoordelijkheden en plichten aangaande:

1. het gebruik van de ICT-middelen:
    - in goede toestand bewaren van de ICT-middelen die ter beschikking gesteld werden
    - niet onbeheerd achterlaten van de ter beschikking gestelde ICT-middelen en het nemen van voldoende veiligheidsmaatregelen om diefstal ervan te verhinderen: bv.
        - Het veilig opbergen van laptops na gebruik.
        - Het plaatsen van een laptopslot indien dit ter beschikking wordt gesteld door het gemeentebestuur.
        - nemen van voldoende veiligheidsmaatregelen die de mogelijkheid tot het inbreken op de systemen van het gemeentebestuur en diefstal van informatie zo klein mogelijk maakt: bv. het activeren van de schermbeveiliging van het werkstation, laptop, smartphone, …
2. de veiligheid van de gegevens die bewaard worden op de systemen:
   het is verboden om de geïnstalleerde virusscanner uit te schakelen tenzij in zeer uitzonderlijke gevallen na uitdrukkelijke toestemming van de IT-beheerder
    - geconfronteerd met een virus, een verdachte e-mail of een verdacht document, moet onmiddellijk contact opgenomen worden met de IT-beheerder die verder de nodige maatregelen neemt om verdere schade te verhinderen.
    - incidenten, eventuele lacunes in de beveiliging van het computersysteem of van methodes die de beveiliging van de gegevens in het gedrang brengen mogen niet aan derden gemeld worden; het uitbuiten van deze zwakheden wordt beschouwd als (poging tot) inbraak.
    - op regelmatige tijdstippen lezen van zijn/haar persoonlijke e-mail van het gemeentebestuur en het opruimen en eventueel archiveren van zijn/haar postbus.

- opslaan van gegevens voor doeleinden van het bestuur moeten bewaard worden op de daarvoor voorziene IT-infrastructuur en niet op de lokale harde schijven of eigen infrastructuur.

3. het doorgeven van persoonsgegevens van derden:
   - Persoonsgegevens van derden worden niet via niet beveiligde externe media doorgegeven.
4. het omgaan met bestanden van onbekende oorsprong: bv.
   - Verdachte bijlagen in e-mails niet openen
   - Onbekende gedownloade bestanden niet openen
   - Onbekende links niet openen
5. het respecteren van de algemene geldende beleefdheidsregels (netetiquette).

3. Ongeoorloofd gebruik

Het gemeentebestuur laat het gebruik van de ICT-middelen niet toe: (deze lijst is ongelimiteerd)

1. om informatie te verspreiden of op te slaan die:
   - het imago, de morele of economische belangen van het gemeentebestuur kan schaden
   - beledigend, lasterlijk, aanstootgevend of discriminerend is
   - schade kan toebrengen aan derden
   - strijdig is met de openbare orde of goede zeden
2. om informatie die als vertrouwelijk wordt betiteld of die wegens de aard ervan redelijkerwijze als vertrouwelijk moet worden beschouwd, zoals bedrijfsgeheimen, persoonlijke gegevens van derden, e.a., door te geven aan personen die niet gerechtigd zijn om deze informatie te ontvangen
3. om onwettige handelingen te stellen door bijvoorbeeld:
   - informatie te verspreiden of op te slaan in strijd met de geldende wetgeving, zoals de wetgeving op de bescherming van de persoonlijke levenssfeer bij de verwerking van persoonsgegevens of in het domein van de elektronische communicatie
   - programmatuur te installeren of te gebruiken waarvoor de bevoegde autoriteit geen toestemming heeft verleend
   - de wetgeving over het auteursrecht en andere intellectuele rechten te schenden (bv. programmatuur te kopiëren tenzij dit door de licentie van de leverancier of door de wet is toegestaan)
   - een valse identiteit aan te nemen op het netwerk
4. om buiten de gevallen van de normale bedrijfscommunicatie massaal ongewenste of ongevraagde elektronische post (spamming) of kettingbrieven te verspreiden
5. om acties te ondernemen die de beveiliging van systemen of informatie in het gedrang kunnen brengen zoals bijvoorbeeld:
   - interne en externe systeem- en netwerkbeveiliging (beveiliging van een computer, netwerk of gebruikersnummer) te omzeilen, zodat o.a. in die systemen kan worden binnengedrongen om de bedrijfszekerheid te ondermijnen of schade toe te brengen
   - schadelijke software (zoals Trojaanse paarden, virussen, wormen, ...) op de systemen van het gemeentebestuur te ontwerpen, te installeren en/of andere gebruikers aan te zetten deze software te gebruiken
   - niet-geëigende en ongeoorloofde toegang te forceren tot systemen waartoe men niet gerechtigd is
   - het netwerk af te luisteren
   - om andere gebruikers te storen bij het uitoefenen van hun activiteiten of pogingen te ondernemen om eender welke dienst, netwerk of computer te verstoren (een netwerk of computer overbelasten, pogingen om een systeem te doen falen, …)
   - om systeeminformatie, systeemconfiguratie, toepassingsprogramma's of bestanden te wijzigen, te verwijderen of door te geven aan derden, indien men daarvoor uit hoofde van zijn functie niet is gerechtigd

- om ICT-apparatuur die geen eigendom is van het gemeentebestuur, aan te koppelen zonder toestemming van de IT-beheerder
- om intern ontwikkelde programmatuur, die deel uitmaakt van het patrimonium van het gemeentebestuur en die binnen het kader van de beroeps- of opleidingsactiviteit werd ontwikkeld, te commercialiseren voor persoonlijke doeleinden. Handelingen stellen die het verder gebruik of de exploitatie van de software kunnen hinderen tenzij het programmatuur betreft die specifiek werd ontwikkeld om onbeperkt te worden verspreid zoals bijvoorbeeld programmatuur met een open broncode licentie.
- voor persoonlijk gebruik buiten de gevallen die onder Hoofdstuk 5 “Persoonlijk gebruik” van deze policy zijn toegestaan.

Zonder limitatief te zijn, mag de ICT-infrastructuur van het gemeentebestuur voor de volgende zaken enkel gebruikt worden als dit gebeurt in functie van de uitvoering van de opdracht van het personeelslid:

1. om muziek-, radio- of televisieprogramma’s te beluisteren/bekijken via het internet.
2. om deel te nemen aan chatrooms of newsgroups.
3. voor het spelen van computerspelletjes.
4. voor zaken met winstgevend doel.

4. Wachtwoorden en loginnamen

Toegang tot de computerinfrastructuur en het netwerk wordt verleend door individuele authenticatie. De loginnaam moet beschermd worden met een goed gekozen wachtwoord. Voor wachtwoorden gelden de volgende regels:

1. het wachtwoord moet binnen een termijn van vijf dagen nadat men hiertoe wordt uitgenodigd, worden gewijzigd en in elk geval onmiddellijk als dit door de IT-beheerder gevraagd wordt (bv. na vaststelling van een inbraak of wanneer het wachtwoord te zwak is).
2. niemand mag zijn wachtwoord aan derden (bv. collega’s, jobstudenten, stagiairs, consulenten, …) doorgeven en/of door derden laten gebruiken en niemand mag de loginnaam van een ander gebruiken.
3. wachtwoorden van anderen proberen te kraken of te achterhalen is verboden.
4. het is niet toegelaten om wachtwoorden in zichtbare (bv. Post-it) vorm op te slaan.
5. er dient omzichtig omgegaan te worden bij het ingeven van wachtwoorden (bv. niet als iemand toekijkt).
    - Alle draagbare computers die vertrouwelijke informatie over het gemeentebestuur bevatten, moeten worden beschermd, bijvoorbeeld met een opstart-wachtwoord en een schermbeveiliging om de inhoud van de gegevens zo optimaal mogelijk te beveiligen.
    - Toegangsrechten moeten worden verleend volgens de need-to-have en need-to-know-principes.
    - Hierbij krijgt een (interne en externe) gebruiker standaard enkel de toegangsrechten die noodzakelijk zijn voor de functionele rol van de gebruiker binnen de organisatie.
    - Wanneer men merkt dat men toegang heeft tot informatie waarvoor men niet gemachtigd zou moeten zijn, moet de werknemer dit onmiddellijk melden bij de ICT-verantwoordelijke zodat de toegangen beperkt kunnen worden.
    - Iedere gebruiker is verantwoordelijk en aansprakelijk voor alles wat onder zijn/haar loginnaam en wachtwoord gebeurt.

5. Persoonlijk gebruik

Het gemeentebestuur laat binnen redelijke perken het persoonlijke gebruik toe van het gemeentebestuur – ICT-middelen.
Onder toegelaten persoonlijk gebruik van ICT-middelen binnen redelijke perken wordt verstaan dat:

1. anderen door dit gebruik niet mogen gestoord worden bij de uitoefening van hun beroepsactiviteiten;
2. er behoudens andere afspraken geen kosten aan verbonden zijn voor het gemeentebestuur;
3. het persoonlijke gebruik van de ICT-middelen geen nadelige invloed heeft op de individuele arbeidsprestaties volgens het overeengekomen arbeidsrooster.

Het gemeentebestuur heeft het recht om, wanneer dit om bedrijfsredenen vereist is of wanneer dit wettelijk bepaald is:
1. de voorwaarden voor het ter beschikking stellen van ICT-middelen te herzien en eventueel te beperken
2. de gemaakte kosten voor persoonlijk gebruik op de gebruiker te verhalen
3. de verloren arbeidstijd aan te rekenen.

6. Printergebruik

Het bestuur stelt printers ter beschikking waarmee documenten kunnen afgedrukt en in sommige gevallen ook ingescand of gekopieerd worden. Aangezien sommige printers op plaatsen staan die toegankelijk zijn voor derden, zodat deze mogelijk ook vertrouwelijke informatie kunnen inkijken, zijn op dit vlak ook enkele richtlijnen nodig.

- Zo houdt men zich eraan om niet onnodig documenten af te drukken, zeker niet als er vertrouwelijke of gevoelige gegevens op staan.
- Indien de printer niet beveiligd is met een persoonlijke code, dienen documenten direct van de printer worden afgehaald bij het afdrukken.
- Bij het kopiëren of inscannen van documenten dienen de documenten onmiddellijk van het toestel te worden afgehaald en terug veilig op geborgen te worden.
- Indien documenten worden ingescand en het toestel niet toelaat om de betreffende documenten op de juiste plaats te zetten zodat toegang wordt beperkt tot enkel deze die hier toegang toe mogen hebben, dient men na het inscannen zo snel mogelijk de documenten manueel op de juiste plaats te zetten en te verwijderen uit de map met ingescande documenten. Dit kan door ze naar jouw eigen mailbox toe te zenden.

7. Gebruik van e-mail

Voor de meeste werknemers stelt het bestuur een e-mailadres ter beschikking. De werknemer dient een aantal vuistregels in acht te nemen omtrent het gebruik van dit e-mailadres:

- Stuur geen professionele e-mailberichten door naar je persoonlijk e-mailadres. Zo zou je immers organisatiegegevens buiten de organisatie brengen met het gevolg dat deze gegevensstroom niet meer onder controle is.
- Open geen verdachte e-mails waarvan je de afzender niet kent.
- Klik niet op bijlages van verdachte e-mailberichten.
- Open geen bijlages van e-mails met gebrekkig Nederlands.
- Klik niet op linken in e-mails met gebrekkig Nederlands.
- Klik niet op linken in e-mails waarvan je de afzender niet kent.
- Kijk eerst goed na of je de schrijfwijze van de naam van afzender van het bericht kent.
  Voorbeelden:
  - 2dehanbs.be is niet hetzelfde als 2dehands.be
  - Mail van noreply@knp.com maar link in de mail (als je hierover beweegt met je muis, NIET op klikken, dan zie je dat de link helemaal niet gaat naar een KPN website)
- Verstuur geen e-mailberichten via open netwerken aangezien hier geen beveiliging is voorzien. Je kan hier gemakkelijk afgeluisterd worden.
- Indien je e-mailberichten kan raadplegen via je smartphone, installeer dan zeker een antivirustoepassing.

Wat indien je merkt dat er toch een virus of verdachte gedragingen zijn op je toestel:

- Trek de netwerkkabel uit
- Zet je wifi uit
- Ontkoppel al jouw netwerkschijven (Doe dit echter enkel indien je over de nodige kennis hiertoe beschikt!)
- Contacteer onmiddellijk de ICT-helpdesk zodat zij tijdig kunnen ingrijpen en de schade nog kunnen beperken.
- Neem contact op met leden van de informatieveiligheidscel
- Ga zeker niet in op boodschappen om te betalen voor het terug ter beschikking stellen van bestanden.

Omgang met bijlages:

- Bewaar bijlages uit een e-mail op de fileserver indien deze belangrijke en/of vertrouwelijke informatie bevat
- Bewaar de bijlage op de fileserver op een plaats waar dat de nodige personen er aan kunnen.
- Indien de tekst van het mailbericht geen belangrijke inhoud bevat kan deze worden verwijderd
- Indien de tekst van het mailbericht wel belangrijke inhoud bevat kan je deze ook eventueel opslaan op de fileserver.
- Na de bovenstaande acties kan de betreffende e-mail worden verwijderd uit de mailbox zonder dat er informatie verloren gaat.
- Indien je bestanden intern wil delen, gebruik dan enkel de verwijzing naar het bestand op de fileserver. Op deze manier verhinder je dat mensen met een verkeerde versie van het bestand werken en verminder je ook het dataverkeer binnen de organisatie.

8. Controle & Sancties

Binnen de wettelijke grenzen kan het gemeentebestuur controle uitoefenen op gegevens die een gebruiker opslaat, verstuurt of ontvangt binnen het toepassingsgebied van deze policy. Dit past binnen de opdracht van het gemeentebestuur en haar doelstellingen:

- het voorkomen van ongeoorloofde of lasterlijke feiten, feiten die strijdig zijn met de goede zeden of die de waardigheid van een andere persoon kunnen schaden
- de bescherming van de belangen van de organisatie
- de veiligheid en/of de goede technische werking van de netwerk-informaticasystemen, met inbegrip van de controle op de eraan verbonden kosten, alsook de fysieke beveiliging van de installaties van de organisatie
- de naleving van de principes en gebruiksregels voor het gebruik van online technologieën zoals vermeld in deze policy

De controle zal gebeuren op een wijze die de inmenging in de persoonlijke levenssfeer zoveel als mogelijk vermijdt en daar waar het niet anders kan tot een minimum beperkt.

IT-beheerders mogen elke controle uitvoeren die inherent is aan het beheer van informatiesystemen en netwerken, om de goede werking ervan te waarborgen of om overbelasting of veiligheidsproblemen te voorkomen of te verhelpen.

Indien ernstige vermoedens ontstaan van misbruik of onregelmatigheden, dan kan de gemeentesecretaris de IT-dienst de opdracht geven de gegevens te verwerken om ze aan een geïdentificeerde of identificeerbare persoon toe te schrijven.

Gegevens of communicatie waarvan niet uitdrukkelijk is aangegeven dat het gaat om privé-informatie, kunnen op elk moment door de gemeentesecretaris worden ingekeken.

Privécommunicaties kunnen bij ernstig vermoeden van misbruik of van niet-naleving van de policy gecontroleerd worden op hun aantal, tijdstip en/of hun inhoud mits in kennisstelling van de betrokken gebruiker.

Het resultaat van de controle zal ter kennis van het personeelslid worden gebracht.
Indien een personeelslid zich niet aan deze richtlijnen houdt, kan deze schuldig worden bevonden en worden er al dan niet sancties getroffen.
De mogelijke sancties of tuchtmaatregelen staan beschreven in de van toepassing zijnde rechtspositieregeling en/of het arbeidsreglement.

B. Aanvullende gedragslijn voor het gebruik van internet en e-mail in de gemeentelijke basisschool voor het onderwijzend personeel

I. Inleiding

De personeelsleden van de Gemeentelijke Basisschool zijn gebonden aan de regels voor elektronische post en internet, die door de het gemeentebestuur/schoolbestuur werden opgesteld. Onderstaand protocol vat deze regels samen en vervolledigt daar waar nodig, gezien het bijzonder karakter van de dienst 'onderwijs'.

II. Algemene principes rond het gebruik van internet en e-mail

A. Professioneel gebruik

- U krijgt beschikking over internet en e-mail enkel voor professioneel gebruik ter ondersteuning van onderwijskundige taken en als didactisch hulpmiddel bij het nastreven van de eindtermen ICT.
- Als algemene regel is de grootste voorzichtigheid geboden om school-gerelateerde zaken te versturen via e-mail. Het is immers niet altijd veilig vertrouwelijke informatie via de elektronische post te bezorgen. U mag uw verbinding niet gebruiken voor zaken die schade kunnen toebrengen aan de Gemeentelijke Basisschool.
- U mag geen bedreigende, intimiderende, en discriminerende - zoals racistische of seksistische - boodschappen versturen. Boodschappen van politieke of commerciële aard die geen verband houden met de uitoefening van uw functie zijn eveneens verboden. Wanneer u dergelijke berichten ontvangt, dient u deze onmiddellijk en definitief te wissen.

B. Opvolging/registratie van het gebruik van internet en e-mail

1. Het schoolbestuur kan het algemeen internetgebruik (lijst van geraadpleegde sites) en elke overdracht van gegevens via de elektronische post (verzendings- en bestemmingsadres, tijdstip van verzending) opvolgen. Zij kan uitsluitend de ICT-coördinator hiermee gelasten. Inhoud van e-mails is niet raadpleegbaar.
2. Deze opvolging van gegevens gebeurt met het oog op de netwerkplanning, om veiligheidsredenen of om het gebruik van internet en de elektronische post te evalueren.
3. Het schoolbestuur zal geen systematische controles uitvoeren op het individueel gebruik dat u maakt van internet en e-mail.
4. Enkel indien er aanwijzingen zijn die doen vermoeden dat er misbruik wordt gemaakt van dit instrument, kan er effectief een controle worden uitgevoerd op het individuele gegevensverkeer en kunnen er sancties volgen.
5. De registratie en eventuele bewaring van gegevens is onderworpen aan de Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens en gebeurt uitsluitend om bovenvermelde redenen.
6. De wet van 8 december 1992 geeft u een recht van toegang tot en van verbetering van de door de werkgever bewaarde informatie. Om inzage te verkrijgen in de gegevens die over u worden bijgehouden, dient u zich te richten tot het schoolbestuur.

C. Gebruikersidentificatie

In gevallen waarbij Uw toegang tot internet en e-mail persoonlijk is geregistreerd is iedereen verantwoordelijk voor alles wat onder zijn gebruikersidentificatie gebeurt. In zulke gevallen is het verboden:

- om uw eigen usernaam en paswoord door te geven aan derden,
- om het e-mailadres van iemand anders te gebruiken,
- om uw identiteit als verzender of het e-mailadres van verzending te proberen verhullen.

III. Internet

De personeelsleden kunnen vrij gebruik maken van de elektronische communicatiemiddelen van de school met de volgende beperkingen:

- Het downloaden en installeren van software (shareware – payware – freeware) of andere uitvoerbare bestanden via het internet is toegelaten indien dit noodzakelijk is voor de uitoefening van uw functie. U neemt contact op met de ICT-Coördinator die zal nagaan of er geen operationele of contractuele implicaties zijn en/of de software niet reeds aanwezig is.
- Het is verboden te surfen op sites met voor kinderen onaanvaardbaar materiaal. Men moet er rekening mee houden dat er steeds sporen en links kunnen achterblijven die door volgende gebruikers ongewenst kunnen worden gezien.
- Indien het nodig is om bij het surfen een login en/of paswoord te gebruiken zorgt men er voor dat deze gegevens niet worden opgeslagen op de computer, zodat eventuele volgende gebruikers zich niet ongewenst kunnen aanmelden.
- Het raadplegen van sociale media (facebook, netlog, twitter, …) gebeurt nooit tijdens de lessen of in aanwezigheid van de kinderen. Bij het verlaten van de werkplek, ook al is het voor korte tijd, vergeet men niet uit te loggen.
- Bij het posten van berichten op de sociale media draagt men er zorg voor dat de integriteit van de school niet wordt geschaad.

IV. E-mail

A. E-mail adres

De elektronische post is een uiterst handige vorm van communicatie. Naargelang de school wordt voor elke computerlocatie (klas), leerkracht of functie een e-mailadres voorzien. Dit adres kan gebruikt worden voor communicatie met de ouders of tussen collega's. Elke titularis wordt geacht deze post regelmatig na te kijken.

Toch besteedt u het best aandacht aan de volgende punten:

- Vraag u telkens af of e-mail wel het meest geschikte medium is voor de boodschap die moet doorgegeven worden. Tijdens een rechtstreeks gesprek krijgt de geadresseerde veel meer informatie dan alleen de letterlijke tekst. Een gedachtewisseling verloopt gemakkelijker en efficiënter via de telefoon of in een persoonlijk gesprek.
- Let erop dat u e-mail pas gebruikt voor zover geen andere afspraken bestaan om uw boodschap via een ander kanaal te communiceren (afspraken rond briefwisseling, verspreiding berichten e.d.).
- Bezorg alleen de relevante informatie aan de bestemmeling. Beperk ook het aantal ontvangers tot die personen waarvan je een reactie verwacht. Personen die louter moeten geïnformeerd worden, ontvangen uw bericht in kopie.

B. Blokkeren:

Mails- zowel ontvangen als verzonden mails- kunnen geblokkeerd worden wanneer zij één van de volgende bestanden als bijlage bevatten:

- uitvoerbare bestanden (met als extensie b.v. .exe, .com, .pif, .scr, .vbs, .eml, bat, …)
- bestanden die omwille van hun grootte capaciteitsproblemen kunnen veroorzaken
- bestanden die virussen bevatten.

Dergelijke mails kunnen niet gedeblokkeerd worden.

C. SPAM:

Ook "spams" kunnen een bedreiging vormen voor het bedrijfsnetwerk. Spamming is het ongevraagd toesturen van berichten, meestal in heel grote hoeveelheden. Het is verboden te antwoorden op dergelijke berichten, zelfs niet met de vraag niets meer te versturen. Spam dient u onmiddellijk te verwijderen.

D. Kettingbrieven:

U mag geen kettingbrieven openen en/of verzenden via e-mail. Kettingbrieven dient u onmiddellijk te verwijderen.

V. Webstek

- Bij het samenstellen van een webstek voor een school is het onvermijdelijk om ook foto's van kinderen en personeel te publiceren. In het kader van het vrijwaren van de privacy zal steeds worden vermeld dat iedereen zich kan verzetten om foto's van zichzelf of van zijn kinderen te tonen. De webmaster zal bij klacht onmiddellijk het desbetreffende materiaal verwijderen. Deze procedure zal ook in het Huishoudelijke Reglement moeten vermeld worden.
- Indien mogelijk zal vooraf toestemming worden gevraagd aan ouders, zowel als aan leerkrachten om gegevens te publiceren, die zouden kunnen inbreuk doen aan de wet op de privacy.
- De inbreng van externen bij het samenstellen van de webstek wordt gestimuleerd en getolereerd voor zover de integriteit van de leerlingen, het personeel en de instelling zelf gerespecteerd wordt. Deze inbreng zal steeds onderhevig zijn aan controle door de webmaster.

VI. Maatregelen bij niet-naleving van de gedragscode

Bij niet-naleving van het protocol kunnen de schoolbesturen van de Scholengemeenschap overgaan tot:

- het intrekken van de toegang tot internet en e-mail
- disciplinaire maatregelen (cfr. Arbeidsreglement)