Aanvulling
‘Begrensd gedrag, naar gedragsregels op school’

Gedragscode voor internet en e-mail

Schooltype	Voortgezet onderwijs.
Doelgroep	Gebruikers van internet (leerlingen, personeel) of intranet (op school of thuis).
Terrein	Gedragscode voor internetfaciliteiten (internet, e-mail, intranet).
Detaillering	De gedragscode bevat onderdelen over gebruik (bijvoorbeeld hoe je e-mails opstelt: zakelijk en in correct Nederlands), wat niet is toegestaan (spammen, hoaxen, openen onbekende attachments, chatten, deelnemen aan kansspelen et cetera), de manier van controle en de sancties bij oneigenlijk gebruik van internetfaciliteiten.
Formulering	De gedragscode wordt op de homepage van de schoolwebsite vermeld. Het is een uitgebreid document van vier pagina’s waarin gedetailleerd staat omschreven hoe internetfaciliteiten gebruikt dienen te worden. Ook staat expliciet beschreven wat niet is toegestaan.
Handhaving	Controles worden regelmatig uitgevoerd door middel van steekproefcontrole op het e-mail-en internetverkeer. Bij verdenking van een gebruiker op oneigenlijk gebruik van internet, volgt de systeembeheerder het internetgedrag van de betreffende gebruiker en rapporteert de schoolleiding hierover in dossiervorm. Afhankelijk van de aard en de ernst van de overtreding worden disciplinaire -of ordemaatregelen getroffen.

Gedragscode internet-en e-mailgebruik

Het Sint-Maartenscollege gevestigd te Maastricht, in deze vertegenwoordigd door de locatiedirecteuren, dhr. J. Moes (locatie VMBO) en mevr. C. Rijgersberg (locatie HAVO/VWO)

en

de gebruiker van de geboden faciliteiten

maken de volgende afspraken over de wijze waarop gebruik gemaakt zal worden van internet en e-mail en hoe omgegaan zal worden met daaruit verkregen tot een persoon herleidbare data.

1. Werkingssfeer

Deze gedragscode geldt voor alle gebruikers van de internetfaciliteiten die door het Sint-Maartenscollege worden geboden. Naast gebruikers van de netwerken in Sint-Maartenscollege zijn deze regels ook van toepassing op gebruikers die thuis of elders gebruik maken van een e-mailadres van de school of een schoolinter-en intranetsite.

Gebruikmaken van de school internetfaciliteiten betekent instemmen met deze gedragscode. De school draagt zorg voor bekendmaking van deze code en eventueel toekomstige aanvullingen en/of wijzingen.

Deze gedragscode is altijd op te vragen via http://www.sint-maartenscollege.nl – *informatie voor leerlingen.*

2. Algemeen

2.1 Het Sint-Maartenscollege kan het recht tot gebruik van (een deel van) internet toestaan, maar ook altijd weer intrekken. Zonder dat recht is gebruik van (een deel van) internet niet toegestaan.

2.2 Het Sint-Maartenscollege behoudt zich het recht voor om de toegang tot bepaalde sites te beperken. Met name sites met een pornografische, racistische en/of discriminerende inhoud kunnen worden geweerd.

3. Gebruik

3.1 Gebruikers mogen internet en e-mail incidenteel en kortstondig voor privédoeleinden gebruiken, zowel intern als extern, voor zover hieraan geen bijzondere kosten verbonden zijn, mits dit niet storend is voor de dagelijkse werkzaamheden en mits hierbij voldaan wordt aan de verdere richtlijnen van deze gedragscode. Het bezoeken van chat-/babbelboxen, het deelnemen aan kansspelen en het spelen of downloaden van spelletjes is niet toegestaan.

De gebruikelijke gedragsregels, zoals de regels die momenteel gelden voor het ondertekenen van schriftelijke correspondentie, het vertegenwoordigen van het Sint-Maartenscollege en voor het verzenden van post, zijn ook van toepassing op e-mail en andere toepassingen.

3.2 De infrastructuur voor elektronische communicatie kent een eigen vorm van kwetsbaarheid en een eigen vorm van beveiliging. Deze vraagt om speciale aandacht op ten minste de volgende punten:

- User-identificatie (inlognaam) en wachtwoord zijn persoonsgebonden en mogen niet aan anderen worden doorgegeven. De gebruiker die zijn/haar user-identificatie en wachtwoord doorgeeft aan derden is aansprakelijk voor de eventuele schade die door misbruik door derden is ontstaan.
- Het downloaden van software en applicaties is niet toegestaan, tenzij vooraf schriftelijk toestemming is verleend door de schoolleiding. Deze toestemming wordt alleen verleend als wordt voldaan aan de geldende rechten en eventuele licenties worden betaald. Gedownloade software en applicaties moeten op virussen zijn gescand voor gebruik.
- Vertrouwelijke gegevens mogen niet zonder toestemming naar buiten worden verstuurd.
- Het is niet toegestaan inkomende privé-berichten te genereren door deel te nemen aan voor het onderwijs/de school niet relevante nieuwsgroepen, abonnementen op e-zines, nieuwsbrieven en dergelijke.
- Onbedoelde inbreuk op beveiliging, van binnenuit of van buitenaf, dient u aan de systeembeheerder te melden.

3.3 E-mail

Om het gebruik van e-mail in goede banen te leiden, het gezicht van het Sint-Maartenscollege naar buiten te beschermen en te voorkomen dat mailservers overbelast raken, gelden de volgende regels:

- Een bericht verstuurd vanaf het school e-mailadres wordt door de ontvanger gezien als een e-mail van het Sint-Maartenscollege. Houd berichten kort en zakelijk en gebruik correct Nederlands, zoals dat ook in schriftelijke communicatie gebruikelijk is.
- Het is niet toegestaan dreigende, seksueel intimiderende, dan wel racistische berichten te versturen.
- Attachment is een bestand (Word, Excel, et cetera) dat meegezonden kan worden. De grootte van de attachments in één e-mailbericht kan nooit meer zijn dan 1 MB, anders wordt het niet verzonden of ontvangen. 1 MB staat ongeveer gelijk aan 250 pagina's tekst.
- Als een mailbox groter wordt dan 20 MegaByte is het niet meer mogelijk om mail te ontvangen, dus met name e-mails met grotere aanhangsels dienen snel verwijderd te worden.
- E-mailfaciliteiten worden door het Sint-Maartenscollege geboden om communicatie efficiënter te laten verlopen. Het zenden en lezen van privé e-mail binnen werktijd dient dan ook vergeleken te worden met het voeren van privé telefoongesprekken binnen werktijd.

Niet toegestaan zijn

- Spammen: het verzenden van e-mail aan grote groepen mensen, die niet om een dergelijk bericht gevraagd hebben. Het versturen van een bericht naar alle medewerkers van het Sint-Maartenscollege is ook een vorm van spam en mag slechts worden uitgevoerd indien er duidelijk een algemeen belang is gediend.
- Hoaxing: het doorsturen van berichten over hoe je snel rijk kunt worden, dat er een bijzonder gevaarlijk virus is of iets met gelukspoppetjes/kettingbrief. Het grootste deel van viruswaarschuwingen die men ontvangt, berust op verzinsels. Bij twijfel over de waarheid van een ingekomen bericht wordt deze uitsluitend naar de systeembeheerder (zijn e-mailadres) gestuurd, die de boodschap op zijn waarde kan schatten en zo nodig andere gebruikers op de hoogte kan stellen.
- Openen van ongevraagde attachments of waarvan de afzender bij de ontvanger onbekend is. De kans is groot dat het hier om een virus gaat. Bij twijfel altijd eerst contact opnemen met de systeembeheerder.

4. Controle

4.1 Om veiligheidsredenen wordt al het inkomende en uitgaande verkeer voor het Sint-Maartenscollege netwerk vastgelegd in zogenaamde logs om, wanneer er iets misgaat, te kunnen zien wat er gebeurd is en de eventuele schade te kunnen vaststellen. Alleen de systeembeheerders en de schoolleiding hebben toegang tot deze logs.

4.2 Om de veiligheid van het netwerk te waarborgen en toe te zien op een zorgvuldig gebruik overeenkomstig deze regeling, worden van tijd tot tijd controles uitgevoerd. Het toezicht op het gebruik zal bestaan uit het steekproefsgewijs controleren van het gebruik van internet en e-mailverkeer. Daartoe kunnen anonieme lijsten van bezochte internetsites en van verstuurde e-mails worden uitgedraaid.

4.3 Binnenkomend internet-en e-mailverkeer wordt zo goed mogelijk gecontroleerd op virussen en soortgelijk ongerief. Mocht blijken dat een e-mailbericht een virus bevat, dan wordt het automatisch tegengehouden en worden de verzender en ontvanger daarover ingelicht. Indien desondanks een e-mailbericht wordt ontvangen dat mogelijk een virus bevat, dan dient de ontvanger onverwijld contact op te nemen met de systeembeheerders.

4.4 Indien een sterke verdenking bestaat dat een gebruiker bovenstaande regels overtreedt, fraude pleegt of zich schuldig maakt aan niet-loyaal gedrag, kan de schoolleiding de systeembeheerder opdracht geven de logs actief te bekijken en het internetgedrag van de betreffende gebruiker in dossiervorm te rapporteren.

4.5 Controleren, alsmede openen van e-mail – ook die voor privégebruik ten behoeve van het opsporen van onrechtmatig gedrag van de werknemer – is in opdracht van de schoolleiding toegestaan indien er sprake is van een redelijke verdenking of een vermoeden van ongeoorloofd handelen.

4.6 De betreffende gegevens worden bewaard zolang dit in het kader van nader onderzoek en eventueel te treffen maatregelen jegens een gebruiker noodzakelijk is.

4.7 De systeembeheerder is altijd gehouden aan een geheimhoudingsplicht.

5. Sancties

Bij handelen in strijd met deze regeling, het schoolbelang of de algemeen geldende normen en waarden kunnen afhankelijk van de aard en de ernst van de overtreding disciplinaire of ordemaatregelen worden getroffen.