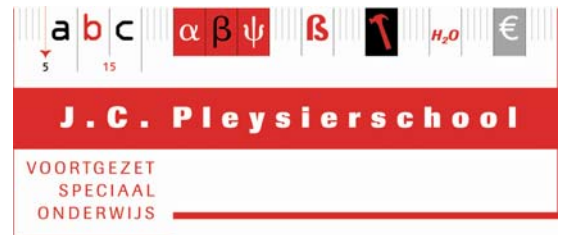


## Gedragsregels Internet



### [Voor Internet, E-mail, etc.]

*Ten behoeve van het uitvoeren van werkzaamheden en van het onderwijsleerproces, voorziet de Stichting J.C. Pleysierschool haar medewerkers en leerlingen van elektronische informatie- en communicatiemiddelen, zoals computers en de daarop geïnstalleerde software, netwerken, e-mail en internet en intranet. Het gebruik van deze middelen brengt steeds grotere risico's met zich mee. Zo kan vertrouwelijke informatie onjuist terecht komen of misbruikt worden of zou ongeautoriseerd toegang tot informatie en gegevens verkregen kunnen worden. De Pleysierschool treft maatregelen om onverantwoord gebruik van deze middelen zoveel mogelijk te voorkomen. Een van die maatregelen is deze set gedragsregels, waarin wordt aangegeven op welke wijze de ter beschikking gestelde informatie- en communicatiemiddelen gebruikt dienen te worden, met als doel een goede balans te vinden tussen een verantwoord en zorgvuldig gebruik en de controle daarop door de Pleysierschool en de bescherming van de privacy van de gebruikers.*

School	Stg. J.C. Pleysierschool, instelling voor Voortgezet Speciaal Onderwijs met diverse locaties in de regio Haaglanden.
Doelgroep	Gebruikers van datanetwerken van de school en internet: Zowel leerlingen als medewerkers.
Terrein	ICT, gedragsregels voor internetfaciliteiten (internet, e-mail, netwerk, etc.).
Detailering	De gedragsregels bevatten onderdelen over gebruik (bijvoorbeeld hoe je e-mails opstelt: zakelijk en in correct Nederlands), wat niet is toegestaan (spammen, hoaxen, openen onbekende bijlagen, chatten, deelnemen aan kansspelen et cetera), de manier van controle en de sancties bij oneigenlijk gebruik van internetfaciliteiten.
Formulering	De gedragsregels worden op de schoolwebsite en intranet vermeld. Het is een uitgebreid document van vijf pagina's waarin gedetailleerd staat omschreven hoe internetfaciliteiten gebruikt dienen te worden. Ook staat expliciet beschreven wat niet is toegestaan.
Handhaving	Controles kunnen regelmatig worden uitgevoerd door middel van een steekproef op het e-mail- en internetverkeer. Bij verdenking van een gebruiker op oneigenlijk gebruik van internet volgt de ict-coördinator het internetgedrag van de betreffende gebruiker en rapporteert de directie hierover in dossiervorm. Afhankelijk van de aard, ernst en dader van een overtreding, worden disciplinaire- of ordemaatregelen getroffen.

*De Stg. J.C. Pleysierschool gevestigd te Den Haag, hanteert 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.*

*Instemming Medezeggenschapsraad: 8 januari 2009*

*Vastgesteld door de Algemene Directie (CvB): 17 maart 2009*

## **1. Werkingsfeer**

Deze gedragsregels gelden voor alle gebruikers van de internetfaciliteiten die centraal door de J.C. Pleysierschool (hierna JCP genoemd) worden geboden. Naast gebruikers van de netwerken op de diverse schoollocaties zijn deze regels ook van toepassing op gebruikers die thuis of elders gebruik maken van een e-mailadres van de school of een internetsite van de school.

Gebruikmaken van de school internetfaciliteiten betekent instemmen met deze gedragsregels. De school draagt zorg voor bekendmaking van deze gedragsregels (via internet) en eventueel toekomstige aanvullingen en/of wijzingen.

## **2. Algemeen**

**2.1** De JCP 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** De JCP behoudt zich het recht voor om de toegang tot bepaalde sites te beperken. Met name het bezoeken van sites met een pornografische, racistische, discriminerende of intimiderende inhoud is verboden. Ook louter op entertainment gerichte sites zijn ongewenst en kunnen worden geweerd.

## **3. Gebruik**

**3.1** In het algemeen geldt dat gebruik, tegenstrijdig aan de doelstelling en identiteit van de school, zowel in persoonlijk gebruik als in relatie tot anderen binnen of buiten de school, niet is toegestaan. Het bezoeken van externe chat/babbelboxen, het deelnemen aan kansspelen, winkelen, het spelen van niet-educatieve spelletjes en op eigen initiatief downloaden van software/applicaties is verboden.

Gebruikers mogen internet 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 dit niet in strijd is met deze gedragsregels.

**3.2** Het is niet toegestaan om identificeerbaar beeld- en/of geluidmateriaal van medewerkers, leerlingen of andere bij de school betrokkenen via elektronische informatie- en communicatiemiddelen bekend te maken, zonder voorafgaande toestemming van betrokkene of diens wettelijke vertegenwoordiger.

Het is bovendien niet toegestaan om vanaf schoolnetwerken door middel van elektronische berichten (bijv. e-mail, msn/message, chat, sms, mms, e.d.):

- informatie anoniem of onder een fictieve naam te versturen
- iemand elektronisch lastig te vallen
- (met opzet) virussen te verspreiden
- dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende berichten en kettingmail berichten te verzenden of door te sturen. Indien u ongevraagde informatie van deze aard aangeboden krijgt, dient u dit te melden bij een (leidinggevende) medewerker van de school
- gebruik te maken van andermans persoonsgegevens.

**3.3** De gebruikelijke gedragsregels (evt. vastgelegd in een statuut), zoals de regels die gelden voor het ondertekenen van schriftelijke correspondentie, het vertegenwoordigen van de JCP (-locaties) en voor het verzenden van post, zijn ook van toepassing op e-mail en andere toepassingen.

**3.4** 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:

- De inrichting van en het onderhoud aan de schoolnetwerken is voorbehouden aan de daartoe aangewezen personen en/of partijen. Beveiligingen mogen niet worden uitgeschakeld, gewijzigd of omzeild. Inbreuk hierop en/of inbraak op de netwerken is niet toegestaan, kan worden aangegeven bij de politie en eventuele schade wordt op de dader(s) verhaald.
- Het gebruik van internet vindt uitsluitend plaats met de door de JCP daarvoor beschikbaar gestelde faciliteiten. Van de infrastructuur van de JCP mag geen gebruik gemaakt worden met behulp van andere dan de ter beschikking gestelde informatie- en communicatiemiddelen. Slechts door de ict-coördinator (namens de directie) goedgekeurde en door systeembeheer beveiligde hardware mag op de schoolse verbindingenetwerken worden aangesloten of verbonden.
- Gebruikeridentificatie (inlognaam) en wachtwoord zijn persoonsgebonden en mogen niet aan anderen worden doorgegeven. De gebruiker die zijn/haar gebruikersnaam en wachtwoord aan anderen verstrekt, is aansprakelijk voor de eventuele schade die door misbruik door derden is ontstaan. Wachtwoorden worden nooit op een 'publieke pc' opgeslagen.
- De gebruiker gaat verantwoordelijk om met (openstaande) netwerkverbindingen, d.w.z. hij laat een pc niet onbeheerd achter wanneer hij daarmee onbevoegden toegang tot diverse netwerkdiensten of -bronnen verschaft.
- Het installeren van software en applicaties is niet toegestaan, tenzij vooraf schriftelijk toestemming is verleend door de directie en verricht onder auspiciën van de ict-coördinator. Deze toestemming wordt alleen verleend als wordt voldaan aan de geldende rechten en eventuele licentiekosten.
- 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, communities, abonnementen op e-zines, nieuwsbrieven en dergelijke.
- Onbedoelde inbreuk op beveiliging, van binnenuit of van buitenaf, dient u aan de locatie ict-er en/of aan de ict-coördinator te melden.

### **3.5 E-mail**

Medewerkers gebruiken uitsluitend (zo mogelijk) het pleysier.net mailadres voor officiële email namens de school. Leerlingen gebruiken (zo mogelijk) ook bij voorkeur het door de school verstrekte mailadres voor schoolse correspondentie.

Om het gebruik van e-mail in het algemeen in goede banen te leiden, het gezicht van de JCP (-locaties) naar buiten te beschermen en te voorkomen dat mail servers overbelast raken, gelden de volgende regels:

- Een bericht verstuurd vanaf het school e-mailadres wordt door de ontvanger gezien als een e-mail van de JCP. Houd berichten kort en zakelijk en gebruik correct Nederlands, zoals dat ook in schriftelijke communicatie gebruikelijk is.
- Uitgaande mail van medewerkers moet altijd worden voorzien van een disclaimer als: "Dit bericht is strikt persoonlijk en slechts bestemd voor de geadresseerde. Indien u dit bericht abusievelijk ontvangt, verzoekt de J.C. Pleysierschool u dit bericht te verwijderen. Er kunnen aan de inhoud van dit bericht geen rechten worden ontleend. Doorzending van het bericht aan derden, in welke vorm ook, wordt niet op prijs gesteld."
- Het is niet toegestaan dreigende, seksueel intimiderende, dan wel racistische berichten te versturen.
- Een bijlage (attachment) is een bestand (Word, Excel, et cetera) dat meegezonden kan worden. De grootte van een bijlage in één e-mailbericht is beperkt (10 MegaByte in 2009), anders wordt het niet verzonden of ontvangen. 1 MB staat ongeveer gelijk aan 250 pagina's tekst.
- Als een mailbox groter wordt dan xxx MegaByte (250 in 2009) is het niet meer mogelijk om mail te ontvangen, dus met name e-mails met grotere aanhangsels dienen snel verwijderd of gearchiveerd te worden. Voor archivering dient de H- of G-schijf; niet de (Outlook-)mailbox.

- E-mailfaciliteiten worden door de JCP geboden om zakelijke (en/of educatieve) communicatie efficiënter te laten verlopen. Het zenden en lezen van privé-e-mail binnen werktijd (en/of lestijd) 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 (locaties van) de JCP is ook een vorm van spam en mag slechts worden uitgevoerd, indien er duidelijk een algemeen belang is gediend.
- Hoaxen: het doorsturen van berichten over hoe je snel rijk kunt worden, dat er een bijzonder gevaarlijk virus is of iets met gelukspopetjes/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 ict-coördinator (diens e-mailadres) gestuurd die de boodschap op zijn waarde kan schatten en zo nodig anderen op de hoogte kan stellen.
- Openen van ongevraagde bijlagen 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 locatie ict-er.

## **4. Controle**

**4.1** Om veiligheidsredenen kan al het inkomende en uitgaande verkeer voor het JCP netwerk vastgelegd worden in zogenaamde logs om, wanneer er iets misgaat, te kunnen zien wat er gebeurd is en de eventuele schade te kunnen vaststellen. Alleen systeembeheer (en via deze, de ict-coördinator) heeft 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 geanonimiseerd 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 –zo mogelijk- de verzender en ontvanger daarover ingelicht. Indien desondanks een e-mailbericht wordt ontvangen dat mogelijk een virus bevat, dan dient de ontvanger direct contact op te nemen met de locatie ict-er en/of ict-coördinator.

**4.4** Indien een sterke verdenking bestaat dat een gebruiker bovenstaande regels overtreedt, fraude pleegt of zich schuldig maakt aan niet-loyaal of ontoelaatbaar gedrag, kan de directie de ict-coördinator opdracht geven om logs te genereren en/of te analyseren (via systeembeheer) en over het internetgedrag van de betreffende gebruiker in dossiervorm te rapporteren. Zowel het bestuur als de betrokkene worden hiervan op de hoogte gesteld.

**4.5** Controleren, als mede openen van e-mail – ook die voor privégebruik ten behoeve van het opsporen van onrechtmatig gedrag van de werknemer – is in opdracht van de directie dus 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, met een maximum bewaartermijn van 6 maanden.

**4.7** De ict-coördinator en het personeel van systeembeheer zijn in deze altijd gehouden aan een geheimhoudingsplicht.

## **5. Sancties**

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

## 6. Slot

In alle gevallen waarin deze gedragsregels niet voorzien, beslist de directie conform het arbeidsrechtelijke kader, (evt. leerlingenstatuut) en de Wet bescherming persoonsgegevens.

### **Toelichting**

School: Stichting J.C. Pleysierschool (JCP), bij de KvK geregistreerd onder nummer 41155107.

Algemene directie (directie): Voorganger van het College van Bestuur, met gemandateerde bevoegdheden.

College van Bestuur (CvB): Het centrale bestuursorgaan van de school. Het CvB legt verantwoording af aan de raad van toezicht J.C. Pleysierschool. (Met ingang van 01-08-09)

Medewerkers: Hieronder worden verstaan, alle medewerkers met een arbeidsovereenkomst, vakantiekrachten, stagiaires, vrijwilligers, ingeleende medewerkers, zoals uitzend- en freelance krachten, telewerkers en externe consultants.

Leerling: Jeugd- of jongere die bij de J.C. Pleysierschool is ingeschreven, dan wel op andere wijze aan (een deel van) het schoolprogramma deelneemt.

Locatie ict-er: De contactpersoon –op locatie- voor hardware en netwerk-zaken (loci).

Ict-coördinator: De schoolbrede beleidsmedewerker voor ict (Centraal Bureau).

Systeembeheer: De (externe) uitvoeringsorganisatie voor systeem- en netwerkbeheer.

© J.C. Pleysierschool