Aan: Iedereen
Van: Directie
Betreft: Gedragscode internet- en e-mailgebruik
Datum: maart 2019

SECVO, handelend onder de naam Christiaan Huygens College, gevestigd te Eindhoven, in deze vertegenwoordigd door de directeur-bestuurder, drs. M.B. van den Berg, en de medezeggenschapsraad van de instelling, 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 Christiaan Huygens College worden geboden. Naast gebruikers van de netwerken in de locaties van de scholen zijn deze regels ook van toepassing op gebruikers die thuis of elders gebruikmaken van een e-mailadres van de school of een school inter- en intranetsite. Gebruik maken van de school internetfaciliteiten betekent instemmen met deze gedragscode. De school draagt zorg voor bekendmaking van deze code en eventuele toekomstige aanvullingen en/of wijzingen. Deze gedragscode is op te vragen via de website en/of de elektronische leeromgeving van de school.

2. Algemeen

2.1 Het Christiaan Huygens College 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 Christiaan Huygens College behoudt zich het recht voor om de toegang tot bepaalde sites te beperken. Met name sites met een pornografische, racistische, discriminerende inhoud kunnen worden geweerd.

3. Gebruik

3.1 Gebruikers mogen internet en e-mail incidenteel en kortstondig voor privé doeleinden 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. De gebruikelijke gedragsregels, zoals de regels die momenteel gelden voor het ondertekenen van schriftelijke correspondentie, het vertegenwoordigen van het Christiaan Huygens College 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 tenminste de volgende punten:

- user-identificatie (inlognaam) en wachtwoord zijn persoonsgebonden en mogen niet aan anderen worden doorgegeven;
- het downloaden van software en applicaties is niet toegestaan, tenzij vooraf schriftelijk toestemming is verleend door de systeembeheerder van de locatie. Deze toestemming wordt alleen verleend als wordt voldaan aan de geldende rechten en evt. 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 e.d.
- Onbedoelde inbreuk op beveiliging, van binnen uit of van buitenaf, dient u aan de systeembeheerder te melden.

Niet toegestaan is:

- 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 Christiaan Huygens College 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 van de locatie gestuurd die de boodschap op zijn waarde kan schatten en zo nodig andere gebruikers op de hoogte kan stellen.
- Phishing: Het versturen van berichten naar ontvangers met het doel wachtwoorden en/of kritieke informatie van anderen te achterhalen.
- Openen van ongevraagde attachments of waarvan de afzender niet in de bijgaande e-mail vermeldt wat het voorstelt. De kans is groot dat het hier om een virus gaat. Bij twijfel altijd eerst contact opnemen met de systeembeheerder van de locatie.

4. Controle

4.1 Om veiligheidsredenen wordt al het inkomende en uitgaande verkeer voor het Christiaan Huygens College netwerk vastgelegd in zogenaamde logs om, wanneer er iets misgaat, te kunnen zien wat er gebeurd is en de evt. schade te kunnen vaststellen. Alleen de systeembeheerder en de directie hebben toegang tot deze logs. Van tijd tot tijd kunnen controles plaatsvinden.

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 Binnenkomende 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 systeembeheerder van de locatie.

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 directie 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 privé gebruik ten behoeve van het opsporen van onrechtmatig gedrag van de werknemer is 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.

Aldus overeengekomen en ter goedkeuring ondertekend door de medezeggenschapsraad op 2019.