



Protocol e-mail-, netwerk- en internetgebruik

Artikel 1 Definities, doel en werking

1. Dit protocol bevat een regeling voor het gebruik van het computernetwerk, e-mail en internet door medewerkers en extern adviseurs van CVO en leerlingen, medewerkers en extern adviseurs van de CVO-scholen.
2. Het protocol is opgesteld conform de Wet Bescherming Persoonsgegevens.
3. Doel van het protocol:
Het protocol bevat regels en afspraken over het computergebruik door medewerkers, leerlingen, extern adviseurs, stagiairs en uitzendkrachten van CVO of CVO-school (hierna gebruikers genoemd) en over de manier waarop CVO omgaat met het registreren, verzamelen en monitoren van tot een persoon herleidbare data inzake het gebruik van hardware, software, e-mail en internet. Doelstelling hiervan is een goede balans te vinden tussen een verantwoord gebruik van internet en e-mail en bescherming van de privacy van gebruikers op de werkplek.
4. Het protocol geldt voor alle in artikel 3.1 genoemde gebruikers die gebruik maken van het netwerk van CVO of een CVO-school en voor medewerkers en leerlingen die vanaf een andere locatie (een CVO-school of huisadres) gebruik maken van het netwerk van CVO of van een CVO-school.
5. Het protocol behelst e-mail-, netwerk- en internetgebruik. Hieronder wordt ieder gebruik van de door CVO of een CVO-school geboden faciliteiten verstaan: het gebruik van het CVO of school-netwerk, het gebruik van het zakelijke e-mailadres en het gebruik maken van toegang tot internet.

Artikel 2 Algemene uitgangspunten

1. Gegevens die tot een persoon herleidbaar zijn, zullen niet worden geregistreerd, verzameld, gecontroleerd, gecombineerd dan wel bewerkt, anders dan in dit protocol is afgesproken.
2. Persoonsgegevens zullen alleen gebruikt worden voor het doel waarvoor ze verzameld zijn.
3. Het registreren van gegevens die tot een persoon herleidbaar zijn wordt tot het minimum beperkt. Hierbij wordt gestreefd naar een maximale bescherming van de privacy van de gebruikers op de werkplek.
4. Indien dit uit een oogpunt van noodzakelijk te verrichten werkzaamheden onvermijdelijk is, is het aan het beheer van het netwerk toegestaan om persoonlijke data van gebruikers tijdelijk ontoegankelijk te maken. Anders dan in acute noodsituaties, worden gebruikers tijdig op de hoogte gebracht van deze tijdelijke ontoegankelijkheid.

Artikel 3 Algemene bepalingen t.a.v. gebruikers

1. Alle medewerkers van CVO (met een vast of tijdelijk dienstverband, stagiairs en uitzendkrachten) en leerlingen van de CVO-scholen hebben toegang tot het computernetwerk. Tevens kan het wenselijk zijn dat een gast (bijv. een extern adviseur)

van CVO of van een CVO-school gebruik kan maken van het computernetwerk. Hiervoor dient tijdig een, door een staflid getekend, verzoek te worden ingediend bij de afdeling ICT. De voor het gebruik noodzakelijke gebruikersnaam, wachtwoord en eventueel e-mailadres worden door de afdeling ICT verstrekt.

2. De eerste keer dat een gebruiker gebruik maakt van het computernetwerk wordt beschouwd als de totstandkoming van een overeenkomst tussen CVO of een CVO-school en de gebruiker met betrekking tot dit protocol computergebruik, waarbij de gebruiker instemt met de in dit protocol verwoorde regels en afspraken.
3. Het recht om gebruik te maken van het computernetwerk vervalt zodra iemand geen medewerker meer is van CVO of leerling of medewerker van een CVO-school zoals beschreven in artikel 3 punt 1.
4. Het computernetwerk kan door gebruikers worden benaderd op daartoe ingerichte werkplekken.

Artikel 4 E-mail- en internetgebruik medewerkers en gasten

1. Alle gebruikers van het netwerk mogen het e-mailsysteem en de toegang tot internet kortstondig voor niet-zakelijk (persoonlijk) verkeer gebruiken voor het ontvangen en versturen van persoonlijke e-mailberichten zowel intern als extern, mits dit niet storend is voor de dagelijkse werkzaamheden, voor anderen en het de goede werking van het netwerk niet verstoort.
2. Het recht van de gebruiker om persoonlijke e-mailberichten te ontvangen en versturen is gebonden aan de voorwaarde dat het niet is toegestaan dreigende, seksueel intimiderende, racistische dan wel andere berichten te versturen welke in strijd zijn met de identiteit van CVO.
3. CVO of een CVO-school behoudt zich het recht voor de toegang tot bepaalde sites te beperken en/of te verbieden. Met name sites met een pornografische, racistische, discriminerende of op entertainment gerichte inhoud kunnen worden geweerd.
4. Medewerkers van de afdeling ICT van CVO of van een CVO-school zullen in principe niet de inhoud van zowel persoonlijke als zakelijke e-mailberichten lezen. Gegevens over het aantal e-mails, de e-mailadressen en andere data hieromtrent worden wel geregistreerd, voor zover dat vereist is i.v.m. wettelijke of contractuele verplichtingen vanuit het optreden als provider (Telecommunicatiewet). Dit laat onverlet dat controles op incidentele basis (steekproef) of vanwege een zwaarwichtige reden kunnen plaatsvinden. Hiervan wordt altijd vooraf melding gemaakt bij de directie door (een medewerker van) de afdeling ICT.
5. Voor het gebruik van e-mail geldt verder:
 - Alleen het e-mailadres dat door de organisatie is toegewezen aan de gebruiker mag worden gebruikt. Bij communicatie via e-mail moet herleidbaar zijn wie de afzender is.
 - De afzender is verantwoordelijk voor een juiste adressering van zijn of haar informatie.
 - De normale gedragsregels, die gelden voor schriftelijke correspondentie (zoals correct taalgebruik) zijn ook van toepassing op e-mail en andere toepassingen (zoals nieuwsgroepen).
 - Alle regels voor elektronische informatie gelden tevens voor bijlagen.
 - Formele informatie per e-mail dient conform de CVO-huisstijl of conform de huisstijl van de CVO-school te worden opgesteld.
 - Verzending van vertrouwelijke informatie of gevoelige informatie via e-mail is niet toegestaan.
 - Alle elektronisch verzonden informatie dient een disclaimer te bevatten.

Artikel 5 Gedragsregels / bewust zijn van de risico's van internetgebruik

1. Het internet is een open infrastructuur die voor iedereen toegankelijk is. De gebruiker moet zich ervan bewust zijn dat de betrouwbaarheid (beschikbaarheid, integriteit en exclusiviteit) van informatie op het internet niet altijd gewaarborgd is en dat alle activiteiten die de gebruiker op internet ontplooit, bekeken en vastgelegd kunnen worden door vele partijen. Berichtgeving die gevoelige informatie of persoonsgegevens, zoals bedoeld in de Wet Bescherming Persoonsgegevens, mag niet per e-mail of internet

worden verzonden, mits dit gebeurt via een veilige, gecodeerde verbinding. Verder vraagt de kwetsbaarheid van de infrastructuur van internet om speciale aandacht op tenminste de volgende punten:

- * gebruikersnaam (inlognaam) en wachtwoord zijn persoonsgebonden en mogen niet aan anderen worden doorgegeven; de geregistreeerde gebruiker is verantwoordelijk voor alle acties die met behulp van zijn/haar gebruikersnaam worden uitgevoerd;
- * het downloaden van grote bestanden en/of applicaties is niet toegestaan, tenzij vooraf schriftelijke toestemming is verleend door de verantwoordelijke en een medewerker van de afdeling ICT. Deze toestemming wordt alleen verleend als eventuele licenties worden betaald en als wordt voldaan aan de geldende rechten. Aanschaf en gebruik van nieuwe software dient vooraf met een medewerker van de afdeling ICT besproken te worden.
- * van buiten het netwerk komende bestanden moeten op virussen zijn gescand voor gebruik en mogen niet in strijd zijn met auteursrechtelijke voorschriften.
- * vertrouwelijke gegevens en bedrijfsgevoelige informatie mogen niet zonder toestemming buiten de organisatie worden verstuurd. Iedere gebruiker wordt geacht het vertrouwelijke karakter en de bedrijfsgevoeligheid van gegevens te onderkennen.

Zie tevens artikel E4 van de CAO. In geval van twijfel wende men zich tot de direct leidinggevende.

2. Het is niet toegestaan inkomende privé-berichten te genereren door deel te nemen aan niet-zakelijke nieuwsgroepen, abonnementen op e-zines, nieuwsbrieven en dergelijke; onbedoelde inbreuken op beveiliging, van binnenuit of vanuit de buitenwereld, dient aan een medewerker van de afdeling ICT gemeld te worden.

Het is in het bijzonder niet toegestaan op internet:

- * sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten;
- * pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal dat op de een of andere manier in strijd is met de grondslagen van CVO te bekijken, te downloaden of te verspreiden;
- * spelletjes en muziekbestanden te downloaden, uit te wisselen of uit te voeren, te winkelen, te gokken, deel te nemen aan kansspelen en/of chat-/babbelboxen te bezoeken, tenzij zoiets past in het kader van onderwijsactiviteiten;
- * zich ongeoorloofd toegang te verschaffen tot niet-openbare bronnen op het netwerk van CVO of van de CVO-school of het internet;
- * opzettelijk informatie waartoe men via het netwerk en/of internet toegang heeft verkregen zonder toestemming te veranderen of te vernietigen.

Indien ongevraagd informatie die voldoet aan bovengenoemde beschrijvingen wordt aangeboden, dient dat aan een medewerker van de afdeling ICT gemeld te worden.

Het is bovendien niet toegestaan om door middel van e-mail:

- * berichten anoniem of onder een fictieve naam te versturen; dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende berichten en ketting-e-mailberichten te verzenden of door te sturen;
- * iemand elektronisch lastig te vallen.

Het is ook op een andere manier niet toegestaan op internet in strijd met de wet of onethisch te handelen.

3. De gebruiker verplicht zich het werkstation waarop hij/zij gewerkt heeft dan wel tijdelijk verlaat, te blokkeren of af te sluiten teneinde het ongeautoriseerde gebruik van het netwerk te voorkomen.

Aan het einde van een werkdag dient de computerapparatuur op de werkplekken uitgeschakeld te worden.

Artikel 6 Controle

1. Om de veiligheid van het netwerk te waarborgen en toe te zien op een zorgvuldig gebruik in overeenstemming met deze regeling, worden van tijd tot tijd controles uitgevoerd. Daarnaast wordt toegezien op de technische integriteit en beschikbaarheid van de infrastructuur en diensten. Het toezicht op het gebruik bestaat uit het periodiek en steekproefsgewijs controleren van het gebruik van internet en e-mailverkeer

- (tijdsbesteding, sites die bezocht worden). Daartoe kunnen lijsten van bezochte internetsites en van verstuurde e-mail worden uitgedraaid.
2. Binnenkomend e-mailverkeer wordt zo goed mogelijk gecontroleerd op virussen en soortgelijk ongerief. Indien een e-mailbericht een virus bevat dan wordt dat bericht automatisch tegengehouden. Verzender en ontvanger worden zomogelijk daarover ingelicht. Indien desondanks een e-mail wordt ontvangen dat mogelijk een virus bevat, dan dient de ontvanger zo snel mogelijk contact op te nemen met de helpdesk van CVO of een CVO-school.
 3. Indien mocht blijken dat in strijd met deze regeling wordt gehandeld of indien daarvoor aanwijzingen zijn (zoals klachten, signalen van binnen of buiten de organisatie en systeemstoringen), kunnen gegevens van de betrokken gebruiker(s) worden uitgedraaid, bekeken en gebruikt. De betreffende gegevens worden maximaal zes maanden bewaard, of zolang dit in het kader van nader onderzoek en eventueel te treffen maatregelen tegen een gebruiker noodzakelijk is.
 4. Voor zover noodzakelijk worden derden ingeschakeld bij onderzoek en controlewerkzaamheden.
 5. Medewerkers van de afdeling ICT kunnen tijdens de dagelijkse werkzaamheden (kopieerslagen, back-up, restore, reparaties) data zien van een gebruiker. De medewerkers gaan hier op passende wijze voorzichtig en vertrouwelijk mee om.

Artikel 7 Sancties

In eerste instantie geldt hier het reglement van de organisatie (school of bureau). Onderstaande tekst geeft richtlijnen hoe ten aanzien van ICT-gebruik bij overtredingen gehandeld kan worden. Bij handelen in strijd met deze regeling, het schoolbelang of de algemeen geldende normen en waarden voor het gebruik van het netwerk, internet en e-mail, kunnen afhankelijk van de aard en de ernst van de overtreding maatregelen worden getroffen. Voor medewerkers van CVO gaat het eventueel om disciplinaire en arbeidsrechtelijke maatregelen zoals berisping, overplaatsing, schorsing of beëindiging van de arbeidsovereenkomst. Voor leerlingen geldt het schoolreglement. Voor leerlingen zijn maatregelen denkbaar als tijdelijke of permanente ontzegging van de toegang tot het netwerk of tot internet. Daarnaast kunnen voor leerlingen ook maatregelen getroffen worden zoals schorsing op grond van overtreding van de huis- en orderegels als bedoeld in het schoolreglement. De meest vergaande sanctie voor leerlingen is verwijdering van de school. Voor gasten zijn maatregelen denkbaar als tijdelijke of permanente ontzegging van de toegang tot het netwerk of tot internet. Het is medewerkers van de afdeling ICT toegestaan om verboden, niet-zakelijk of aanstootgevend materiaal bij wijze van voorlopige maatregel, direct te blokkeren. In geval van dreigende storing door gebrek aan opslagcapaciteit is het aan medewerkers van de afdeling ICT toegestaan om verboden, niet-zakelijk of aanstootgevend materiaal (zoals ook amusementsdata, computerspelletjes e.d.) zonder toestemming van de gebruiker te verwijderen.

Artikel 8 Rechten van de gebruikers

Op grond van de Wet Bescherming Persoonsgegevens hebben betrokkenen ten aanzien van de verwerking van persoonsgegevens de navolgende rechten:

1. Inzagerecht: betrokkenen hebben het recht de over hem of haar aanwezige data in te zien. Schriftelijke verzoeken om inzage bij de directie worden binnen twintig werkdagen ingewilligd.
2. Kopierecht: betrokkenen hebben het recht van de over hem of haar aanwezige data een kopie te ontvangen van de directie binnen twintig werkdagen.
3. Correctierecht: betrokkenen hebben het recht om feitelijk onjuiste gegevens uit de aanwezige data te (laten) verbeteren of aan te vullen. Over verzoeken van correctie of aanvulling wordt binnen twintig werkdagen beslist door de directie na overleg met (een medewerker van) de afdeling ICT. Indien een verzoek tot correctie of aanvulling wordt ingewilligd, wordt de correctie terstond uitgevoerd.
4. Verwijderingsrecht: elke medewerker heeft het recht de over hem of haar aanwezige data die niet (langer) terzake doen of in strijd zijn met dit protocol of een wettelijk voorschrift, te laten verwijderen of vernietigen. Over een verzoek om verwijdering en vernietiging wordt binnen twintig werkdagen beslist door de directie na overleg met (een medewerker van)

de afdeling ICT. Indien een dergelijk verzoek wordt ingewilligd, vindt de verwijdering of vernietiging direct plaats.

Artikel 9 Inwerkingtreding en citeertitel

Dit aangepaste protocol is *op 14 maart 2007* vastgesteld door de voorzitter van de Raad van Bestuur van CVO op advies van het Management Team van CVO en treedt in werking met ingang van *1 april 2007*. Dit reglement treedt in de plaats van eerdere voorschriften en aanwijzingen en kan worden aangehaald als "Protocol e-mail, netwerk- en internetgebruik".

Artikel 10 Slotbepaling

In alle gevallen waarin deze regeling niet voorziet, beslist de directie na overleg met (een medewerker van) de afdeling ICT.

Versie 2007, 1.0, 14 maart 2007