



- datum besluit College van Bestuur: 16-10-2006
- datum positief advies managementoverleg: 12-10-2006
- datum inwerkingtreding: 17-10-2006
- geldigheidsduur: onbepaalde tijd

Doel protocol

Het protocol bevat regels en afspraken omtrent computergebruik door medewerkers en leerlingen van de scholen van de Willibrord Stichting en omtrent de wijze waarop de scholen van de Willibrord Stichting omgaat met het registreren, verzamelen en monitoren van tot een persoon herleidbare data omtrent e-mail- en internetgebruik. Doelstelling hiervan is een goede balans te vinden tussen een verantwoord gebruik van internet en e-mail en bescherming van de privacy van medewerkers en leerlingen op de werkplek c.q. op de studieplek.

N.B. Waar hij staat, kan uiteraard ook zij worden gelezen.

Artikel 1: Werkingssfeer

Deze regeling geldt voor een ieder die voor de scholen van de Willibrord Stichting werkzaam is dan wel als leerling is ingeschreven aan de scholen van de Willibrord Stichting.

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 medewerkers op de werkplek.
4. Indien zulks 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

Artikel 3: Algemene bepalingen ten aanzien van leerlingen

1. Ieder die als studerende staat ingeschreven bij de leerlingenadministratie van de scholen van de Willibrord Stichting heeft toegang tot het computernetwerk. De voor het gebruik noodzakelijke gebruikersnaam, wachtwoord en mailadres worden door het systeembeheer verstrekt.
2. De eerste keer dat de leerling gebruikmaakt van het computernetwerk, zal dat worden beschouwd als de totstandkoming van een overeenkomst tussen de scholen van de Willibrord Stichting en de leerling met betrekking tot het computergebruik, waarbij de leerling instemt met de in dit protocol verwoorde regels en afspraken.
3. Het recht om gebruik te maken van het computernetwerk vervalt zodra iemand niet meer ingeschreven staat bij de scholen van de Willibrord Stichting.
4. Het computernetwerk kan door leerlingen worden gebruikt op daartoe ingerichte werkplekken.
5. Het is niet toegestaan te eten en/of te drinken nabij computers.
6. Leerlingen dienen zich te houden aan de aanwijzingen van de medewerkers van de scholen van de Willibrord Stichting.

Artikel 4: E-mailgebruik

1. Medewerkers en leerlingen zijn gerechtigd het emailsysteem kortstondig voor niet-zakelijk (persoonlijk) verkeer te gebruiken voor het ontvangen en versturen van persoonlijke berichten, zowel intern als extern, mits dit niet storend is voor hun dagelijkse werkzaamheden of voor anderen.



2. Het recht van de medewerker en de leerling om persoonlijke mailberichten te ontvangen en versturen is gebonden aan de voorwaarde dat het niet is toegestaan dreigende, intimiderende, seksueel getinte, pesterige, treiterende dan wel racistische of discriminerende berichten te versturen dan wel berichten te versturen die een gewelddadig of beledigend karakter hebben.
3. De scholen van de Willibrord Stichting zullen niet de inhoud van zowel persoonlijke als zakelijke mailberichten lezen. Gegevens omtrent het aantal mails, de mailadressen en andere data hieromtrent worden wel geregistreerd, voor zover zulks vereist is in verband met wettelijke of contractuele verplichtingen vanuit het optreden als provider op grond van de Telecommunicatiewet. Dit laat onverlet dat controles op incidentele basis (steekproef) of vanwege een zwaarwichtige reden kunnen plaatsvinden. Hiervan wordt melding gemaakt bij de functionaris bescherming persoonsgegevens.
4. De normale gedragsregels, zoals die gelden voor schriftelijke correspondentie (zoals correct taalgebruik), zijn ook van toepassing op e-mail en andere toepassingen (zoals nieuwsgroepen).

Artikel 5: Internetgebruik

1. Werknemers en leerlingen zijn gerechtigd kortstondig het internetsysteem voor niet-zakelijk respectievelijk niet-onderwijsgebonden (persoonlijk) verkeer te gebruiken, mits dit niet storend is voor hun dagelijkse werkzaamheden of voor anderen.
2. De scholen van de Willibrord Stichting zullen geen persoonsgegevens over internetgebruik, zoals tijdsbesteding en bezochte sites, registeren en/of controleren, tenzij zulks voortvloeit uit verplichtingen als provider op grond van de Telecommunicatiewet. Dit laat onverlet dat controles op incidentele basis (steekproef) of vanwege een zwaarwichtige reden kunnen plaatsvinden. Hiervan wordt melding gemaakt bij de functionaris bescherming persoonsgegevens.
3. De scholen van de Willibrord Stichting behouden zich het recht voor om de toegang tot bepaalde sites te beperken. Met name sites met een pornografische, racistische, discriminerende of een op entertainment gerichte inhoud zullen worden geweerd.
4. De scholen van de Willibrord Stichting kunnen het recht op gebruik van (een deel van) internet toestaan, maar ook altijd weer intrekken. Zonder dat recht is gebruik van (een deel van) internet niet toegestaan.
5. Het raadplegen van nieuwsgroepen en sites die gericht zijn op discriminatie, racisme, pornografie, beledigingen en extreme uitingen die aanstootgevend kunnen zijn dan wel die oproepen tot geweld, zijn verboden.

Artikel 6: Gedragsregels

1. 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:
 - a. Gebruikersnaam (inlognaam) en wachtwoord zijn persoonsgebonden en mogen niet aan anderen worden doorgegeven. De geregistreerde gebruiker is verantwoordelijk voor alle acties die met behulp van zijn gebruikersnaam worden uitgevoerd.
 - b. Het downloaden of kopiëren van software en applicaties is niet toegestaan, tenzij vooraf schriftelijke toestemming is verleend door de verantwoordelijke of de beheerder. Deze toestemming wordt alleen verleend als wordt voldaan aan de geldende rechten en eventuele licenties worden betaald. Gedownload software en applicaties moeten op virussen zijn gescand voor gebruik. Er mag niet gehandeld worden in strijd met auteursrechtelijke voorschriften.
 - c. Vertrouwelijke gegevens en bedrijfsgevoelige informatie mogen niet zonder toestemming buiten de organisatie worden verstuurd.
 - d. Het is niet toegestaan op enige wijze lessen of anderszins ingeroosterde activiteiten te beperken of te hinderen. Tijdens deze lessen en activiteiten is in de betreffende ruimte individueel computergebruik niet mogelijk.



- e. De gebruiker wordt aanbevolen zelf zorg te dragen voor het maken van een eigen veiligheidskopie.
 - f. De scholen van de Willibrord Stichting zijn niet aansprakelijk voor verlies van data of voor de schade die de gebruiker lijdt in geval van (tijdelijke) onbereikbaarheid van de bestandsopslag of voor schade welke de gebruiker mogelijk lijdt als gevolg van het (tijdelijk) niet bereikbaar zijn van het computernetwerk.
 - g. Het is niet toegestaan zonder toestemming andere computers en/of netwerken binnen te dringen (ook wel "hacken" genoemd). Dit geldt voor systemen binnen en buiten de scholen van de Willibrord Stichting.
 - h. De scholen van de Willibrord Stichting zijn niet aansprakelijk voor mogelijke onjuiste adviezen die haar medewerkers aan de gebruikers geven, dan wel verkeerde interpretaties door de gebruiker van de gegeven adviezen, noch voor eventueel hieruit voortvloeiende schade, waaronder gevolgschade.
 - i. De scholen van de Willibrord Stichting zijn niet aansprakelijk c.q. verantwoordelijk voor verlies van data veroorzaakt door technische storingen bij de scholen van de Willibrord Stichting, dan wel andere interne of externe storing indien dit is veroorzaakt door overmacht. De scholen van de Willibrord Stichting raden gebruikers aan een back-up exemplaar van alle bestanden te bewaren. De gebruiker vrijwaart de scholen van de Willibrord Stichting van elke aansprakelijkheid die mogelijk zou kunnen ontstaan door informatie en activiteiten die de gebruiker op het computernetwerk en/of het internet plaatst en/of ontplooit. De gebruiker wordt expliciet gewezen op het feit dat overtredingen van buitenlandse wetten en regels (met name die van de USA) met betrekking tot het internet- en e-mailgebruik, kunnen leiden tot ernstige strafrechtelijke gevolgen bij bezoek aan landen waar deze wetten en regels van toepassing zijn.
2. Het is niet toegestaan inkomende privé-berichten te genereren door deel te nemen aan niet-zakelijke nieuwsgroepen, abonnementen op niet-zakelijke E-zines, nieuwsbrieven en dergelijke. Onbedoelde inbreuken op beveiliging, van binnenuit of vanuit de buitenwereld, dienen aan de systeembeheerder gemeld te worden.
 3. Het is in het bijzonder niet toegestaan om op internet:
 - a. sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten, dan wel die oproepen tot geweld;
 - b. materiaal te bekijken of te downloaden dat pornografisch, racistisch, discriminerend, beledigend of aanstootgevend is dan wel oproept tot geweld;
 - c. films en muziek te downloaden en/of op te slaan;
 - d. spelletjes te downloaden of uit te voeren, te winkelen, te gokken, deel te nemen aan kansspelen en/of chat-/babbelboxen te bezoeken, tenzij zulks past in het kader van zakelijke of onderwijsactiviteiten (zoals bijvoorbeeld ELO);
 - e. zich ongeoorloofd toegang te verschaffen tot niet openbare bronnen op het internet;
 - f. opzettelijk informatie - waartoe men via internet toegang heeft verkregen - zonder toestemming te veranderen of te vernietigen;
 - g. indien ongevraagd informatie van deze aard wordt aangeboden, dient dat aan de ICT-manager gemeld te worden.
 4. Het is bovendien niet toegestaan om door middel van e-mail:
 - a. berichten anoniem of onder een fictieve naam te versturen; dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende berichten en kettingmailberichten te verzenden of door te sturen ongeacht of de ontvanger deze wilde ontvangen;
 - b. iemand elektronisch lastig te vallen zoals het in hoge frequentie en/of grote omvang berichten versturen in de vorm van bijvoorbeeld bulkmail, junkmail, mailbombing, of welke vorm dan ook.
 5. Het is niet toegestaan:
 - a. softwareprogramma's/scripts/commando's te gebruiken, of anderszins activiteiten te ondernemen, welke de beschikbaarstelling van het netwerk aan andere gebruikers op een nadelige wijze zal kunnen beïnvloeden;



- b. processen/programma's op de systemen van de scholen van de Willibrord Stichting te laten lopen als er geen directe verbinding met het systeem is;
 - c. processen/programma's op de systemen van de scholen van de Willibrord Stichting te installeren zonder uitdrukkelijke schriftelijke toestemming van de scholen van de Willibrord Stichting;
 - d. buiten de voorgeschreven wijze om gebruik te maken van het netwerk;
 - e. eigen software te gebruiken (in verband met het gevaar van virussen);
 - f. gebruik te maken van het netwerk zonder op de gebruikelijke manier in te loggen;
 - g. zonder toestemming van de rechtmatige gebruiker mail te verzenden, waarin in de header iemand anders zijn verzend of reply-adres wordt vermeld.
6. De scholen van de Willibrord Stichting zijn gerechtigd zonder voorafgaande bekendmaking het computernetwerk (tijdelijk) buiten gebruik te stellen en/of het gebruik ervan te beperken voor zover dit noodzakelijk is voor het redelijkerwijs benodigde onderhoud en de veiligheid van de systemen.

Artikel 7: Controle

1. 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. Hiernaast wordt toegezien op de technische integriteit en beschikbaarheid van de infrastructuur en diensten. Het toezicht op het gebruik zal bestaan uit het steekproefsgewijs controleren van het gebruik van internet- en e-mailverkeer. Daartoe kunnen lijsten van bezochte internetsites en van verstuurd e-mails worden uitgedraaid.
2. 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 kan dat automatisch tegengehouden worden en worden de verzender en ontvanger daarover ingelicht. Indien desondanks een e-mail wordt ontvangen dat mogelijk een virus bevat, dan dient de ontvanger onverwijld contact op te nemen met de systeembeheerder.
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), dan kunnen gegevens van (de) betrokken gebruiker(s) worden uitgedraaid, bekeken en gebruikt. De betreffende gegevens worden bewaard zolang dit in het kader van nader onderzoek en eventueel te treffen maatregelen jegens een gebruiker noodzakelijk is.
4. Indien en voor zover noodzakelijk kunnen derden ingeschakeld worden bij de werkzaamheden ten aanzien van onderzoek en controle.
5. Een beheerder kan tijdens werkzaamheden (kopieerslagen, back-up, restore, reparaties) data zien met betrekking tot een gebruiker. De beheerder gaat hiermee op passende wijze prudent om. Toegangscodes en wachtwoorden betrekking hebbende op de schoolnetwerken worden strikt vertrouwelijk behandeld en onder geen beding aan derden verstrekt.

Artikel 8: Sancties

1. Bij handelen in strijd met deze regeling, het bedrijfsbelang of de algemeen geldende normen en waarden voor het gebruik van internet en e-mail, kunnen afhankelijk van de aard en de ernst van de overtreding maatregelen worden getroffen.
2. Voor personeel gaat het eventueel om disciplinaire en arbeidsrechtelijke maatregelen zoals berisping, overplaatsing, schorsing en beëindiging van de arbeidsovereenkomst.
3. Voor leerlingen zijn maatregelen denkbaar als ontzegging van de toegang tot het netwerk of tot internet, tijdelijk of permanent, of andere maatregelen zoals schorsing op grond van overtreding van de huis- en orderegels als bedoeld in de Wet op het Voortgezet Onderwijs en in het Leerlingenstatuut.
4. Het is het beheer toegestaan om verboden, aanstootgevend materiaal, bij wijze van voorlopige maatregel, direct te blokkeren. In geval van dreigende storing door gebrek aan opslagcapaciteit is het aan het beheer toegestaan om verboden materiaal (zoals ook amusementsdata,



computerspelletjes, film, muziek, pornografie en dergelijke) zonder toestemming van de gebruiker te verwijderen.

Artikel 9: Rechten van werknemers en leerlingen

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 aanwezige data in te zien. Verzoeken om inzage worden binnen vier weken ingewilligd.
2. Kopierecht: Betrokkenen hebben het recht van de over hem aanwezige data een kopie te ontvangen binnen vier weken.
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 vier weken beslist. Indien een verzoek tot correctie of aanvulling wordt ingewilligd, wordt de correctie terstond uitgevoerd.
4. Verwijderingrecht: betrokkenen hebben het recht om de over de hem aanwezige data, die niet (langer) terzake doen, of in strijd zijn met dit protocol of een wettelijk voorschrift te laten verwijderen en te laten vernietigen. Over een verzoek om verwijdering en vernietiging wordt binnen vier weken beslist. Indien een dergelijk verzoek wordt ingewilligd, vindt de verwijdering en vernietiging terstond plaats.

Artikel 10: Slotbepalingen

1. In alle gevallen waarin dit protocol niet voorziet, beslist het College van Bestuur van de Willibrord Stichting.
2. Op dit protocol is uitsluitend Nederlands recht van toepassing.
3. Geschillen tussen partijen die uit dit protocol voortvloeien, worden voorgelegd aan de terzake bevoegde instantie.
4. Schade aan de scholen van de Willibrord Stichting of derden veroorzaakt kan op de desbetreffende gebruiker verhaald worden.

Artikel 11: Inwerkingtreding en citeertitel

1. Dit protocol is vastgesteld door het College van Bestuur op 16 oktober 2006 en treedt in werking met ingang van 17 oktober 2006.
2. Dit protocol treedt in de plaats van eerdere voorschriften en aanwijzingen en kan worden aangehaald als "protocol pc-gebruik Willibrord Stichting".

AANHANGSEL BIJ PROTOCOL PC-GEBRUIK (swp 0815)

A. Functionaris bescherming persoonsgegevens.

[Artikel 4.3. De scholen van de Willibrord Stichting zullen niet de inhoud van zowel persoonlijke als zakelijke mailberichten lezen. Gegevens omtrent het aantal mails, de mailadressen en andere data hieromtrent worden wel geregistreerd, voor zover zulks vereist is in verband met wettelijke of contractuele verplichtingen vanuit het optreden als provider op grond van de Telecommunicatiewet. Dit laat onverlet dat controles op incidentele basis (steekproef) of vanwege een zwaarwichtige reden kunnen plaatsvinden. Hiervan wordt melding gemaakt bij de functionaris bescherming persoonsgegevens.]

Functionaris bescherming persoonsgegevens is de heer G.M. van Oostrum.

B. Downloaden software

[Artikel 6.1.b. Het downloaden of kopiëren van software en applicaties is niet toegestaan, tenzij vooraf schriftelijke toestemming is verleend door de verantwoordelijke of de beheerder. 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. Er mag niet gehandeld worden in strijd met auteursrechtelijke voorschriften.]

Medewerkers hebben toestemming voor het downloaden van portable software en applicaties (bijv. vanaf de USB-stick) voor zover het gebruik hiervan onderwijskundig of administratief nodig of wenselijk is.

C. Downloaden films en muziek van internet

[Artikel 6.3.c. Het is in het bijzonder niet toegestaan om op internet films en muziek te downloaden en/of op te slaan]

Medewerkers hebben toestemming voor het van internet downloaden en/of opslaan van films en muziek en zijn gerechtigd aan een individuele leerling hiervoor per situatie eenmalig toestemming te geven, in beide gevallen voor zover het gebruik hiervan onderwijskundig nodig of wenselijk is.

D. Controle via lijsten

[Artikel 7.1. 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. Hiernaast wordt toegezien op de technische integriteit en beschikbaarheid van de infrastructuur en diensten.

Het toezicht op het gebruik zal bestaan uit het steekproefsgewijs controleren van het gebruik van internet- en e-mailverkeer. Daartoe kunnen lijsten van bezochte internetsites en van verstuurde e-mails worden uitgedraaid.]

Met een 'lijst' wordt bedoeld: een lijst met adressen. Op de lijst is de inhoud van de mail resp. website niet vermeld.

E. Privacy

[Artikel 7.3. 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), dan kunnen gegevens van (de) betrokken gebruiker(s) worden uitgedraaid, bekeken en gebruikt. De betreffende gegevens worden bewaard zolang dit in het kader van nader onderzoek en eventueel te treffen maatregelen jegens een gebruiker noodzakelijk is.]

Het uitdraaien, bekijken en mogelijk gebruiken van gegevens geschiedt door het systeembeheer in opdracht van het College van Bestuur of de directie van de school, waarbij de regels t.a.v. privacy in acht worden genomen.

F. Geschillen

[Artikel 10.3. Geschillen tussen partijen die uit dit protocol voortvloeien, worden voorgelegd aan de terzake bevoegde instantie.]

De terzake bevoegde instantie is het College van Bestuur resp. een door het College van Bestuur ingestelde commissie.