STICHTING Kindante

ICT - protocol

Versie1.3 , april 2011.

Inhoudsopgave:

Summary

Dit document is een protocol / gedragscode , waarin is vastgelegd,
- hoe er, in welke situatie, omgegaan moet worden met

- Het gebruik van de e-mail en internetfaciliteit op computers in het netwerk van Kindante
- Het gebruik van vaste telefonie in de organisatie van Kindante en
- Het gebruikt van mobiele telefonie in de organisatie van Kindante

- hoe er , in welke situatie, beveiligingscontroles worden uitgevoerd op bovenstaand gebruik.

Het is van zeer groot belang, dat de inhoud van dit document aan alle leerlingen, leerkrachten, ouders, onderwijs ondersteunend personeel, stagiaires en andere gebruikers van het Kindantenetwerk onder de aandacht wordt gebracht.

1. Inleiding

Wat is nieuw ? Wanneer wordt iets als “nieuw” ervaren. Wanneer is “het nieuwe” niet nieuw meer, maar juist heel “gewoon” geworden ?
Kindantescholen zijn wat dat aangaat een weerspiegeling, een “afdruk” van de wereld om ons heen en onze maatschappij, omdat juist kinderen in contact komen met zaken die weliswaar voor ons als “nieuw” worden ervaren, maar voor kinderen nu juist de gewoonste zaak van de wereld zijn.

Het lijkt niet helemaal op een inleiding, op een protocol ICT, maar heeft er wel alles mee te maken : toen we jaren geleden startten met de fenomenen internet en e-mail in onze organisatie , was er duidelijk behoefte aan een protocol, waarin duidelijke afspraken waren opgenomen om misverstanden en misstanden te voorkomen.

Deze afspraken zijn 1 op 1 overgenomen in dit/deze protocol/gedragscode, dat/die is aangevuld met een aantal Kindantebrede afspraken. Afspraken die te maken hebben met het gebruik van “nieuwe” ict-gerelateerde hardware, software en mogelijkheden.

De invoeringsdatum van het “Kindante Protocol ICT” werd vastgesteld op 1 november 2008. Dit protocol is nu, in april 2011 voorzien van een update.
Vanaf 1 juni 2011 kunnen alle medewerkers en kinderen (gebruikers) het protocol inzien en/of meenemen. Het protocol zal via e-mail worden verspreid aan alle scholen en worden geplaatst op de website en het intranet van Kindante.

Uitgangspunt is, dat iedere gebruiker de gelegenheid heeft (gekregen) kennis te nemen van het protocol en op de hoogte is, dat het gedrag kan worden gecontroleerd. Het privé gebruik tijdens arbeidstijd, het bezoeken van aanstootgevende websites en verwante gedragsregels, werd tot nu toe nauwkeurig omschreven in het Internet en e-mail protocol van Kindante.

Waarom dit protocol ?

Ten eerste:
Ons computernetwerk, inclusief VoIP telefonie, Intranet, webmail en/of VPN verbindingen en in toenemende mate het gebruik van webapplicaties (Esis) en het werken vanaf thuislocaties, vraagt om afspraken en regels.

Ten tweede:
zien we in de maatschappij in toenemende mate het gebruik van

- mobiele telefoons (met internettoegang) door kinderen en personeel op basisscholen
- sms services
- een fotocamera en/of videocamera op mobiele telefoonapparatuur,
- publiceren van filmpjes en fotomateriaal op vrij toegankelijke internetsites (You-Tube)
- downloads (Lime Wire, Torrentz)
- opslagcapaciteit en toenemend gebruik van mobiele gegevensdragers (memorysticks, externe harde schijven, Mp3-spelers, I-Pods, I-Pads, I-Phones)
- Social Media zoals Facebook, LinkedIn, Hyves, MySpace, Twitter,
- chatomgevingen (MSN)

Deze gedragscode is ontwikkeld om misbruik van het netwerk en alle zojuist genoemde voorzieningen te voorkomen en bevat de gedrags – en gebruiksregels waaraan alle gebruikers binnen de netwerken van Kindante zich dienen te houden bij het gebruik van computers, het telefoonnetwerk, mobiele telefoons en genoemde voorzieningen.
Duidelijkheid over wat mag en kan bij dit gebruik, is een eerste vereiste om op goede wijze met deze voorziening om te gaan.

Doel van deze gedragscode is:

- handhaving van goede naam en integriteit
- uitdragen van goede waarden en normen
- tegengaan van “ongewenst gebruik”, seksuele intimidatie, discriminatie of ander onacceptabel gebruik;
- het in bescherming nemen van gebruikers
- systeem en netwerkbeveiliging
- kostenbeheersing

Kindante verwacht van gebruikers van netwerken, dat zij rekening houden met het voorgaande en derhalve zorgvuldig omgaan met het ICT-netwerk en alle genoemde voorzieningen op de school en op de werkplek.
Als hoofdregels voor dagelijks gebruik, gelden dan ook:

- gebruik de computer en de (mobiele) telefoon en/of voorzieningen, in principe voor het werk en/of voor onderwijsdoeleinden
- ieder gebruik in strijd met het doel van deze gedragscode is verboden

2. Privacy

Kindante hecht aan privacy van medewerkers en kinderen. Wet – en regelgeving staan toe dat de werkgever controleert op onjuist gebruik dan wel misbruik van bedoelde voorzieningen. Deze controlemogelijkheden staan ook in deze gedragscode beschreven en geven aan op welke wijze en in welke situaties Kindante tot controle kan overgaan. Daarbij is het streven gericht op een goede balans tussen controle en privacybescherming.

3. Werkingssfeer

Deze gedragscode geldt voor alle gebruikers van de computer/telefonienetwerken van Kindante. (b.v. personeelsleden, leerlingen, partners, stagiaires, (hulp)ouders).

4. Beheer

Het netwerk op scholen, wordt in eerste lijn “onderhouden” door de ICT-er op school. Het betreft hier op zeer kleine schaal kunnen uitvoeren van handelingen, die voor het dagelijks gebruik af en toe noodzakelijk zijn.
Op hoofdlijnen geschiedt alle onderhoud remote, door de leverancier/partner van de digitale marktplaats / datacenter: Unilogic. Zo goed als alle Kindantescholen zijn middels een redundant uitgevoerde glasvezelverbinding (100 Mbit aansluitingen) van Ziggo verbonden met het datacenter alwaar de uitgaande verbindingen (2 x 10 Gigabite) continue gemonitord worden.

Als er in dit protocol gesproken wordt over de netwerkbeheerder, dan is Unilogic Networks bedoeld;
In alle andere gevallen wordt “de ICT-er op school” als terminologie gebruikt.

4. Algemene Uitgangspunten

Ieder computernetwerk kent een eigen vorm van kwetsbaarheid en beveiliging. In dit verband worden de gebruikers gewezen op het volgende:

a) user-identificatie (inlognaam en wachtwoord) , zijn persoonsgebonden en mogen niet aan derden worden doorgegeven
b) de inhoud en het onderhoud van de home-directory (het aan de gebruiker beschikbaar gestelde deel van de server) valt volledig onder de verantwoordelijkheid van de gebruiker zelf
c) het up – en downloaden van niet aan onderwijs gerelateerde bestanden is niet toegestaan zonder uitdrukkelijke permissie van de netwerkbeheerder / ICT-er op school; hier wordt dus niet bedoelt het up – of downloaden van bestanden t.b.v. de intranetomgeving
d) een systeem waarop de gebruiker heeft ingelogd moet worden afgesloten bij het einde van het gebruik; een systeem waarop is ingelogd mag door de gebruiker niet onbewaakt worden achtergelaten.
e) iedere gebruiker dient de aanwijzingen van de netwerkbeheerder / ICT-er op school in kwestie op te volgen
f) bij constatering van storingen of andere onregelmatigheden aan computers of het netwerk, inbreuken op beveiliging etc. dient de gebruiker dit terstond aan de netwerkbeheerder of ICT-er op school te melden
g) Het is een gebruiker verboden om :
    - zelf software te installeren zonder toestemming van de netwerkbeheerder/ICT-er op school
    - niet geautoriseerde apparatuur aan te sluiten op het computernetwerk
    - virussen te maken en/of te verspreiden ; hoewel het gehele netwerk ter degen is beveiligd d.m.v. anti-virusprogrammatuur en firewalls, is de kans aanwezig, dat een flexibel ingezet werkstation (b.v. een lap-top) , niet is voorzien van de laatste updates; in dat geval is het verplicht, om eerst het antivirusprogramma te updaten en dan pas gebruik te maken van een in te pluggen gegevensdrager (b.v. usb-stick), om zo het netwerk niet te vervuilen met virussen, die b.v. van thuis zijn “meegenomen”
    - het computernetwerk te gebruiken om toegang te krijgen tot gegevens die niet voor de gebruiker bestemd zijn , dan wel ander strafbaar gedrag; dit geldt in de regel ook voor beheerders van het netwerk, ICT-ers op school, of anderen die als beheerder mogen inloggen
    - opgeslagen bestanden op mobiele gegevensdragers (usb-sticks) die privacygevoelige informatie bevatten, onbeheerd achter te laten, of niet goed genoeg te beschermen tegen verlies of diefstal
    - storingen of andere onregelmatigheden aan de computers of het netwerk zelf te verhelpen
    - op andere wijze te handelen, in strijd met het doel van de gedragscode

5. Gebruik van Internet

a) Gebruikers mogen via het netwerk van Kindante gebruik maken van internet in het kader van de functie-uitoefening of onderwijsactiviteit.
b) Medewerkers mogen incidenteel en kortstondig internet gebruiken voor persoonlijke doeleinden, mits dit geen storende onderbreking vormt van de werkzaamheden.
c) Het is voor gebruikers in ieder geval verboden middels het netwerk van Kindante internet te gebruiken om:
    - te winkelen voor een niet zakelijk doel
    - te gokken of deel te nemen aan kansspelen
    - niet zakelijke nieuwsgroepen of chatboxen te bezoeken
    - websites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten en/of dit materiaal te bekijken of te downloaden
    - aanstootgevende informatie waartoe men via internet toegang heeft verkregen zonder toestemming te downloaden, te veranderen, te verspreiden of te vernietigen
    - afbeeldingen en videocommunities te bezoeken, die privé-materiaal van wereldburgers publiceert (b.v. You-Tube)
    - te mailen met e-mailaccounts anders dan het account van Kindante (Hotmail,Gmail @Home etc.) en/of de MSN te gebruiken
    - Social Media te gebruiken (zoals b.v. Hyves,Twitter, Facebook en MySpace)

    tenzij een van de bovengenoemde zaken een educatief doel dient, of rechtstreeks voorvloeit uit werkzaamheden, die met de functie op school te maken hebben, dan wel met permissie van de direct leidinggevende in kwestie.
d) Het is ten strengste verboden, om auteursrechtelijk beschermde afbeeldingen te downloaden van internetsites, en die vervolgens te publiceren op schoolwebsites, rondschrijven of e-mails.

6. Gebruik van e-mail

a) iedere gebruiker van Kindante kan beschikken over een persoonlijk e-mailadres (leerlingen evt.vanaf groep 5) , om e-mails te ontvangen en te versturen
b) Volwassen gebruikers mogen incidenteel en kortstondig het e-mailsysteem gebruiken voor het ontvangen en versturen van persoonlijke e-mail mits dit geen onderbreking vormt van de werkzaamheden
c) Het versturen van e-mail moet ten allen tijde voldoen aan de volgende voorwaarden: correct taalgebruik en een correcte vermelding van de afzender, een duidelijke en ter zake doende inhoud en een eventueel meegestuurde bijlage met een maximale omvang van 3 MB
d) Het is voor gebruikers in ieder geval verboden middels het netwerk van Kindante de e-mailfaciliteit te gebruiken om:

    - berichten anoniem of onder een fictieve naam te versturen
    - dreigende, beledigende, seksueel getinte, racistische danwel discriminerende berichten te versturen. Indien een gebruiker ongevraagd informatie van deze aard krijgt aangeboden, dient dit te worden gemeld aan de netwerkbeheerder, ICT-er op school of aan de directie van de school
    - kettingmailberichten te versturen
    - niet-zakelijke privé-berichten, publicaties/rondschrijven, e-zins, nieuwsbrieven, power points e.d. (evt. van buiten de organisatie) te versturen
    - iemand elektronisch lastig te vallen
    - op andere wijze te handelen in strijd met het doel van deze gedragscode

e) De gebruiker is verplicht zijn e-mailbox regelmatig op te schonen, door niet relevante e-mails met evt. attachements te verwijderen uit “postvak-in” , “postvak-uit” en “verwijderde items” , teneinde de schijf/opslagcapaciteit (100 Gigabite per school) niet te overbelasten. Met de intrede van digitale fotografie en de scanfaciliteit van onze multifunctionals, neemt het aantal bestanden, ook in mailboxen soms extreem toe. Het is de verantwoordelijkheid van iedere gebruiker van het Kindantenetwerk en eindverantwoordelijkheid van iedere ICT-er op school, om zo effectief mogelijk om te gaan met de beschikbare schijfruimtes.

7. Het gebruik van vaste telefoon

a) Medewerkers van Kindante mogen telefoons van Kindante gebruiken in het kader van functie-uitoefening
b) Medewerkers mogen incidenteel en kortstondig de telefoon gebruiken voor het voeren van privé-gesprekken als daar uit noodzaak aanleiding toe is, mits dit geen onderbrekende storing vormt van de werkzaamheden
c) Voor gebruikers die een mobiel toestel van de werkgever in gebruik hebben geldt bovendien, dat zij zich houden aan de regels die door de werkgever omtrent het gebruik van mobiele telefoons zijn of worden vastgelegd
d) Het is in ieder geval voor gebruikers verboden telefoons van Kindante te gebruiken om:
    - service en amusementsnummers te bellen die beginnen met 0906 en 0909, tenzij dit gebeurt vanuit een schoolse aangelegenheid;
    - internationale nummers te bellen voor privé-doeleinden;

8a. Gebruik van mobiele telefoon (GSM) door medewerkers

a) De mobiele telefoon wordt ingezet, of beschikbaar gesteld, om de mobiele bereikbaarheid van een medewerker te realiseren en dient overwegend voor inkomende telefoongesprekken en berichten.
b) Iedereen die een mobiele telefoon gebruikt, dient terughoudend om te gaan met het voeren van uitgaande telefoongesprekken en berichten via de mobiele telefoon, tenzij dat uit hoofde van de functie noodzakelijk is
c) bij uitgaande gesprekken en berichten dient dan ook het urgente zakelijke karakter voorop te staan en geniet het gebruik van een vaste (VoIP) telefoon altijd de voorkeur
d) Het is een medewerker niet toegestaan om tijdens werktijden een mobiele telefoon te gebruiken om te telefoneren of te smssen, te fotograferen, te filmen, geluidsfragmenten op te nemen, of te surfen op internet, tenzij daarvoor een uitdrukkelijke reden voor is, c.q. autorisatie van een directielid voor is verleend
e) De kosten van het gebruik van een mobiele telefoon van Kindante in het buitenland, worden bij de gebruiker in rekening gebracht, tenzij er sprake is van een aantoonbare dienstreis en de kosten voortkomen uit zakelijk gesprekken

8b. Gebruik van mobiele telefoons door leerlingen

a) een mobiele telefoon van een leerling mag onder schooltijd niet gebruikt worden
b) Het gebruik van een mobiele telefoon is in die gevallen ook van te voren, met opgaaf van reden(en) door de directie van school geautoriseerd
c) Het niet gebruiken van een mobiele telefoon impliceert dus ook het verbod op opnemen van geluidsfragmenten, het nemen van foto's of het maken van video-opnames binnen school, tenzij daarvoor toestemming is gegeven door de directie
d) Zijn er al met toestemming bestanden zoals genoemd in artikel (8c) gemaakt, dan is het publiceren van deze bestanden middels internet of e-mail ten strengste verboden, tenzij daar door alle personen, voorkomend op die bestanden, toestemming is verleend.

9. Monitoring VoIP – telefoonverkeer

a) Monitoring van telefoongebruik vindt slechts plaats in het kader van de doelstelling van de gedragscode, zoals in de inleiding verwoord
b) Het genereren van gegevens uit de Omnivista/Alcatel telefooncentrale (VoIP) vindt in beginsel plaats op het niveau van de Kindanteorganisatie en wordt 1 op 1 gecommuniceerd op schoolniveau; praktisch gezien, worden de gegenereerde gegevens automatisch, per mail, in Pdf-format doorgezet naar de betreffende directie van een VoIPschool met een maandelijkse frequentie
c) De gegenereerde gegevens van de Omnivista/Alcatel telefooncentrale verschaffen inzicht in verkeersgegevens, nooit op inhoud
d) Met verkeersgegevens wordt bedoeld: per toestelnummer (per toestel) kan inzichtelijk worden gemaakt : het aantal uitgaande gesprekken en totale gespreksduur per toestel per maand
e) Ontvangen gesprekken op een toestelnummer zijn niet te monitoren.
f) De directies, waarvan de scholen zijn aangesloten op het (VoIP) telefoonnetwerk, ontvangen maandelijks de gegenereerde gegevens zoals genoemd onder d); het betreft hier een overzicht van het aantal gevoerde gesprekken per toestel in de schoolorganisatie en de totale gespreksduur; pas bij verdenking van zwaar misbruik, b.v. zeer hoge belkosten of extreem veel telefoonverkeer , kan er op verzoek een overzicht worden gegenereerd waarop niet alleen het aantal gesprekken per toestel wordt getoond, maar ook de nummers waar naartoe werd gebeld.

10. Monitoring e-mail verkeer

a) Monitoring van e-mailverkeer vindt slechts plaats in het kader van de doelstelling van de gedragscode, zoals in de inleiding verwoord
b) De netwerkbeheerder/ICT-er op school kan de postbusgroottes van gebruikers in gebruikersstatistieken genereren, om tijdig te kunnen sturen op de capaciteit van schijfruimte
c) Bij de monitoring van e-mail, gaat het over aantallen mails in postvak-in, postvak-uit, item verzonden items en item verwijderde items, of de totale bestandsgrootte van genoemde boxen, nooit over de inhoud
d) Indien de postbus van een gebruiker de maximale grootte overschrijdt, zal de ICT-er op school, in overleg met de gebruiker trachten de postbus op te schonen, opdat de inhoud van de postbus kan worden teruggebracht naar de toegestane omvang
e) De postbusgrootte kan afhankelijk van de functies van personeelsleden worden aangepast
f) E-mails met attachements, die voor meerdere personen in een organisatie tegelijk worden verstuurd geldt: het attachement, een bestand, wordt in het netwerk maar 1 keer centraal opgeslagen, om overvolle dataschijven en mappen van gebruikers (mijn documenten) te voorkomen

11. Monitoring van internetverkeer

a) Monitoring van internetverkeer vindt slechts plaats in het kader van de doelstelling van de gedragscode, door Unilogic Networks, zoals in de inleiding verwoord
b) Internetverkeer wordt uit oogpunt van overdrachtssnelheden continue gemonitord door de netwerkbeheerder Unilogic Networks;
c) Misbruik van internet kan getraceerd worden, als een werkstation in het gehele Kindantenetwerk zorg draagt, voor een red alert, dat veroorzaakt wordt door enorm datatransport tussen het netwerkstation en het World Wide Web; dergelijk misbruik wordt in eerste instantie gecommuniceerd met de beleidsmedewerker van de stichting.
d) Bij de monitoring van misbruik van internet, kan worden nagegaan welke gebruiker wanneer op welk netwerkstation van Kindante, welke website bezoekt

12. Mobiele telefonie, e-mailverkeer en internetgedrag, werk-gerelateerd in de privé situatie

Het is vandaag de dag heel gewoon, dat werknemers thuis “telewerken” , waarmee wordt bedoeld, dat vanuit de privé-situatie, ingelogd kan worden op het netwerk, (Webmail, VPN, Intranet) voor mail en/of bestanden. Hetzelfde geldt voor de Intranetomgeving van de Kindante (“Kindante-Plaza”) en het gebruik van webapplicaties (b.v. Esis) . Ook hier gelden de gedragsregels, zoals in dit communicatieprotocol genoemd m.b.t. inhoud, het algemeen gebruik en omgang met inloggegevens zoals gebruikersnaam en wachtwoorden.
Met klem worden alle gebruikers van het netwerk van Kindante er hier op geattendeerd, om juist in de thuissituatie of op een andere werkplek buiten school of kantoor zeer voorzichtig om te gaan met inloggegevens en wachtwoorden en nooit de p.c. of laptop onbeheerd achter te laten zonder uit te loggen. Denk hierbij aan Uw eigen privacygevoelige informatie, die van Kindante en/of die van kinderen en ouders.
Tevens wordt het werknemers sterk afgeraden, om met kinderen vanuit de privé-situatie te communiceren middels E-mail, en Social Media zoals genoemd: Facebook, LinkedIn, Hyves, MySpace, Twitter, MSN. Er zijn helaas al teveel gevallen bekend, waarin leerkrachten of andere werknemers op onderwijsinstellingen een tè vertrouwelijke band met studenten of leerlingen opbouwen. Dit getuigt niet van een professionele houding c.q. vertrouwensrelatie tussen medewerker en student/leerling.

Dit protocol is nogal theoretisch en wellicht ook technisch van aard; om U een indruk te geven, in welke behoefte dit document zou moeten voorzien, onderstaande vragen uit de praktijk :

- mag een lerares een Mp-3tje voor eigen gebruik in de pauze downloaden, middels het Kindantenetwerk ?
- mag een klassenassistent tijdens lestijd de huisartsenpraktijk raadplegen voor een nieuwe afspraak ?
- mag een leerling met zijn mobiele telefoon een leraar filmen en dit zonder zijn medeweten op U-Tube publiceren ?
- hoe voorzichtig, gaat een gebruiker om, met gegevens van medewerkers, leerlingen en ouders, als al deze gegevens ook via thuis te benaderen zijn (Esis-A, Esis-B, Cito LOVS, Eduscoop, MIS)?
- mag een kind zijn MP-3 spelerbestanden middels de mail verspreiden onder geïnteresseerden op school ?
- mag een kind middels het netwerk van Kindante, You-Tube filmpjes bekijken op internet, terwijl de ouder(s) een kort gesprekje met de leerkracht voert /voeren ?
- mag een leerkracht een wel heel leuk raadseltje in de mail, privé ontvangen, doorzetten naar collega’s op school ?
- mag een ICT-er op school, als beheerder ingelogd, persoonlijke mappen en e-mail van collega leerkrachten openen ?
- mag een leerkracht ’s avonds en in het weekend of tijdens vakantie contact houden met leerlingen op MSN, omdat men elkaar als contactpersonen/MSNners heeft toegevoegd ?
- mag een directielid elektronisch shoppen op internet, als het spullen voor privé-gebruik betreft ?
- mag een ouder met toestemming, op een vast werkstation een memorystick van thuis gebruiken, t.b.v. een presentatie ?

Dit protocol zal indien de ICT-ontwikkelingen daarom vragen geüpdate worden.

Kindante, April 2011.