Gedragscode ICT Kindante

Inhoud

Inleiding

De gedragscode is een document, waarin helder wordt uiteengezet, hoe er, in welke situatie door medewerkers omgegaan dient te worden met:

- Het gebruik van e-mail en internet binnen het netwerk van Kindante
- Het gebruik van vaste telefonie binnen Kindante
- Het gebruik van mobiele (smart)telefonie binnen Kindante
- Data (bestanden) die ontsloten worden binnen het netwerk van Kindante

Hoe er, in welke situatie, beveiligingscontroles kunnen worden uitgevoerd op bovenstaand gebruik. Deze gedragscode geldt voor iedereen die gebruik maakt van het netwerk van Kindante en/of zich in een Kindantelocatie bevindt. In deze gedragscode wordt onder “medewerkers’ verstaan:

- Medewerkers met een arbeidsovereenkomst
- Stagiaires
- Uitzend – en freelancekrachten
- Vrijwilligers
- Ouders
- Leerlingen
- Externen

Waarbij opgemerkt, dat de ICT-er, dan wel directie van een schoollocatie verantwoordelijk zijn voor het communiceren van deze gedragscode naar stagiaires, uitzend – freelancekrachten, vrijwilligers, ouders, leerlingen en externen die gebruik willen maken van het netwerk op de betreffende locatie.

Uitgangspunt is, dat iedere medewerker van Kindante de gelegenheid krijgt kennis te nemen van betreffende gedragscode. In de maatschappij zien we in toenemende mate het gebruik van:

- Smarttelefoons en tablets (met internettoegang) door kinderen en personeel op basisscholen
- Sms services , WhatsApp , pingen, berichten via social media
- 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, tablets, smartphones)
- Social Media zoals Facebook, LinkedIn, Hyves, MySpace, Twitter
- Chatomgevingen (Skype)

Duidelijkheid over wat mag en kan bij betreffende maatschappelijke ontwikkelingen is een vereiste om op een goede wijze om te gaan met deze voorzieningen.

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 medewerkers van het netwerk, dat zij rekening houden met het voorgaande en derhalve zorgvuldig omgaan met het ICT-netwerken alle genoemde voorzieningen op de school en op de werkplek.

Als hoofdregel voor dagelijks gebruik, geldt 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 niet toegestaan.

1. Privacy

Kindante hecht aan privacy van medewerkers en kinderen. De Wet op de persoonsbescherming staat toe dat de werkgever controleert op onjuist gebruik dan wel misbruik van bedoelde voorzieningen. Deze controlemogelijkheden staan beschreven in betreffende gedragscode 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.

2. 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 noodzakelijk zijn. Op hoofdlijnen geschiedt alle onderhoud, door Unilogic.
Indien er in deze gedragscode gesproken wordt over de netwerkbeheerder, dan wordt Unilogic Networks bedoeld. In alle andere gevallen wordt “de ICT-er op school” als terminologie gebruikt.

3. Algemene Uitgangspunten

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

- User-identificatie (inlognaam en wachtwoord) , zijn persoonsgebonden en mogen niet aan derden worden doorgegeven
- Het wordt aanbevolen om wachtwoorden elke drie maanden te veranderen
- 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, die deze voorziening zakelijk gebruikt
- 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 bedoeld het up – of downloaden van bestanden t.b.v. de intranetomgeving
- 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. Bij het verlaten van werkplek , wordt m.b.v. snel toets combinatie windowstoets - L, de toegang tot het netwerk vergrendeld
- Iedere gebruiker dient de aanwijzingen van de netwerkbeheerder/ICT-er op school in kwestie op te volgen
- Bij constatering van storingen en/of andere onregelmatigheden aan computers of het netwerk, inbreuken op beveiliging etc. dient de gebruiker dit terstond aan de netwerkbeheerder of ICT-er school te melden.

Het is verboden voor een gebruiker 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 laptop) , 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
- Of op andere wijze te handelen, in strijd met het doel van deze gedragscode

NB: het gebruik van memorysticks/usb-sticks wordt uit oogpunt van veiligheid afgeraden (verlies/diefstal). Alle data en outlookcomponenten zijn remote benaderbaar en bevinden zich in de eigen "Kindantecloud" en worden daar veilig geback-upt.

4. Gebruik van Internet

- Gebruikers mogen via het netwerk van Kindante gebruik maken van internet in het kader van de functie-uitoefening of onderwijsactiviteit
- Medewerkers mogen incidenteel en kortstondig internet gebruiken voor persoonlijke doeleinden, mits dit geen storende onderbreking vormt van de werkzaamheden
- Het is verboden, om auteursrechtelijk beschermde afbeeldingen (gedownload van internet) te gebruiken op websites, in rondschrijven of e-mails
- 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 het Skype mail adres 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 voortvloeit uit werkzaamheden, die met de functie op school te maken hebben, dan wel met permissie van de direct leidinggevende in kwestie.

5. Gebruik van e-mail

- Iedere gebruiker van Kindante kan beschikken over een persoonlijk e-mailadres (leerlingen evt. vanaf groep 5) , om e-mails te ontvangen en te versturen
- 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
- 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
- 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 dan wel 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, nieuwsbrieven, power points e.d. (evt. van buiten de organisatie) te versturen
- Iemand elektronisch lastig te vallen (de ontvanger wenst van de verzender geen mail te ontvangen)
- Op andere wijze te handelen in strijd met het doel van deze gedragscode
- De gebruiker is verplicht zijn e-mailbox regelmatig op te schonen, door niet relevante e-mails met evt. attachements te verwijderen uit “postvak-in” , “verzonden items” en “verwijderde items” , teneinde de schijf/opslagcapaciteit 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 Kindante netwerk, om zo effectief mogelijk om te gaan met de beschikbare schijfruimte

6. Het gebruik van vaste telefoon

- Medewerkers van Kindante mogen telefoons van Kindante gebruiken in het kader van functie-uitoefening
- Medewerkers mogen incidenteel en kortstondig de telefoon gebruiken voor het voeren van privégesprekken als daar uit noodzaak aanleiding toe is, mits dit geen onderbrekende storing vormt van de werkzaamheden
- 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 privédoeleinden

7. Gebruik van zakelijk ter beschikking gestelde mobiele telefoon (GSM) c.q. abonnement

- De zakelijk ter beschikking gestelde mobiele telefoon c.q. het abonnement wordt ingezet, of beschikbaar gesteld, om de mobiele bereikbaarheid van een medewerker te realiseren en dient overwegend voor inkomende telefoongesprekken en berichten
- Iedereen die een zakelijke mobiele telefoon c.q. het abonnement 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
- 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
- Het is een medewerker toegestaan om een ter beschikking gestelde mobiele telefoon c.q. het abonnement te gebruiken om te telefoneren of te smssen, te pingen, WhatsApp te gebruiken, te fotograferen, te filmen, geluidsfragmenten op te nemen, of te surfen op internet, als daar werk gerelateerd behoefte aan is
- 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 zakelijke gesprekken

8. Gebruik van mobiele telefoons door leerlingen of ouders

- Een mobiele telefoon van een leerling mag onder schooltijd niet gebruikt worden, tenzij dit een onderwijskundig doel dient en geautoriseerd is door de directie van school
- Het niet gebruiken van een mobiele telefoon impliceert dus ook (voor ouders) 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
- Zijn er al met toestemming bestanden zoals genoemd in artikel (8b) 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 voor is verleend

9. Monitoring VoIP – telefoonverkeer

- Monitoring van telefoongebruik vindt slechts plaats in het kader van de doelstelling van de gedragscode, zoals in de inleiding verwoord
- Het genereren van gegevens uit de VoIP - centrale 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, Pdf-formaat doorgezet naar de betreffende directie van een VoIP school met een maandelijkse frequentie
- De gegenereerde gegevens van VoIP verschaffen inzicht in verkeersgegevens, nooit op inhoud
- Met verkeersgegevens wordt bedoeld: per toestelnummer kan inzichtelijk worden gemaakt: het aantal uitgaande gesprekken en totale gespreksduur per toestel per maand
- Ontvangen gesprekken op een toestelnummer zijn niet te monitoren
- 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

- Monitoring van e-mailverkeer vindt slechts plaats in het kader van de doelstelling van de gedragscode, zoals in de inleiding verwoord
- De netwerkbeheerder/ICT-er op school kan de postbusgroottes van gebruikers in gebruikersstatistieken genereren, om tijdig te kunnen sturen op de capaciteit van schijfruimte
- Bij de monitoring van e-mail, gaat het over aantallen mails in postvak-in, verzonden items en verwijderde items, of de totale bestandsgrootte van genoemde boxen, nooit over de inhoud
- 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
- De postbusgrootte kan afhankelijk van de functies van personeelsleden worden aangepast;
- E-mails met attachements, die voor meerdere personen in een organisatie tegelijk worden verstuurd geldt: het attachment, een bestand, wordt in het netwerk maar 1 keer centraal opgeslagen, om overvolle dataschijven en mappen van gebruikers te voorkomen; het geniet ten alle tijden de voorkeur, om bestanden van deze aard te delen op de data schijf , dan wel op Intranet-omgeving (Boekenkast)

11. Monitoring van internetverkeer

- Monitoring van internetverkeer vindt slechts plaats in het kader van de doelstelling van de gedragscode, door Unilogic Networks, zoals in de inleiding verwoord
- Internetverkeer wordt uit oogpunt van overdrachtssnelheden continue gemonitord door de netwerkbeheerder Unilogic Networks, in het kader van performance-checks
- Misbruik van internet kan getraceerd worden, als een werkstation in het gehele Kindante-netwerk 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 opgemerkt door Unilogic Networks en gecommuniceerd met de beleidsmedewerker van de stichting, die dit oppakt met de leidinggevende van de desbetreffende Kindantelocatie
- 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 “telewerken”, waarmee wordt bedoeld, dat vanuit de privé-situatie, ingelogd kan worden op het netwerk t.b.v. mail en/of het bewerken van bestanden. Bovendien worden steeds meer web applicaties gebruikt (b.v. Esis, website van school, Intranet) . Ook hier gelden de gedragsregels, zoals in deze gedragscode 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 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 collega’s, kinderen en ouders. Ook hier het advies, om wachtwoorden iedere drie maanden te veranderen.

13. Richtlijnen voor het gebruik van Social Media

Social media, met name Twitter, Facebook, Hyves, LinkedIn en You Tube, zijn niet meer weg te denken uit onze maatschappij en dus ook niet bij iedereen die betrokken is bij scholen/onderwijs. Uitgangspunt hierbij is, dat de professionals zelf weten, hoe hiermee verstandig om te gaan. Het digitale gedrag op social media wijkt niet af van het real life gedrag binnen onze scholen.

Algemeen:

- Medewerkers van Kindante delen kennis en andere waardevolle informatie
- Medewerkers maken bij werk gerelateerde onderwerpen duidelijk, of zij op persoonlijke titel of b.v. namens de school publiceren
- Medewerkers van Kindante publiceren geen vertrouwelijke informatie op Social Media
- Medewerkers van Kindante gaan niet in discussie met een ouder of leerling op social media
- Medewerkers van Kindante zijn altijd vertegenwoordiger van een school/stichtingsbestuur, ook als zij een privé mening verkondigen. Bij twijfel: niet publiceren
- Medewerkers van Kindante zijn persoonlijk verantwoordelijk voor wat zij publiceren
- Medewerkers van Kindante weten, dat publicaties op Social media altijd vindbaar zijn (en vaak blijven)

Bij twijfel over een publicatie of over raakvlakken met een school of de stichting, zoeken medewerkers contact met hun leidinggevende.

In de praktijk:

- Ben voorzichtig in de “digitale omgang” met leerlingen op Social Media
- Als je (Hyves, LinkedIn of Facebook) -pagina openbaar is, kan je toekomstig werkgever deze bekijken. Sterker nog, volgens het College Bescherming Persoonsgegevens (CPB) hebben werkgevers daar alle recht toe aangezien de informatie via social media en Google openbaar is. Gebruikmaken van deze informatie in het gesprek zonder dat te vermelden is niet netjes, maar mogelijk
- Verantwoordelijkheid hoofdregel: het gedrag van leraren op Hyves, Facebook, Youtube en Twitter wijkt niet af van wat in de klas of op school gebruikelijk is
- Don’ts: Foto’s of filmpjes van leraren op vakantie of in beschonken toestand op een feest, tweets van leraren die eindigen met …”en nu wel aan je huiswerk. Laterzz XXX…”, te populair taalgebruik en schuttingtaal
- Het gebruik van social media gebeurt ‘real time’. Een druk op de knop en jouw bericht staat direct online. Online informatie die misschien wel eeuwig online staat. Het is niet altijd gemakkelijk om informatie naderhand te (laten) verwijderen. Bedenk dus goed hoe je wilt overkomen in tekst, beeld en geluid – en niet alleen voor dat ene moment
- Werkgevers, leerlingen en ouders zoeken soms op google naar meer informatie. Het is een ongeschreven regel om eenmaal geplaatste berichten niet te verwijderen. Met een druk op de knop (real time) worden ook foute berichten online geplaatst
- Probeer de eerste te zijn om je eigen fouten te corrigeren, zonder eerdere berichten per definitie te wijzigen of te verwijderen. Vermeld daarbij dat jij degene bent die het bericht wijzigt. Geef bij verwijdering een goede reden
- Hou rekening met het wettelijk vastgelegde auteurs-, beeld- en citaatrecht. Het is verboden om zonder toestemming van de maker andermans werk te publiceren. Schending van deze wet levert je een boete op van honderden euro’s
- Sociale omgangsvormen online net zo goed gelden als offline. Respecteer degene tot wie je je richt. Laster, beledigingen en obsceniteit zijn niet geoorloofd. De privacy van anderen wordt gerespecteerd. Dit geldt voor zowel schoolbesturen, directies, onderwijspersoneel als voor leerlingen

- Reageer zoveel mogelijk inhoudelijk op stukken van anderen. Alleen je mening geven, zonder onderbouwing daarvan, vervuilt de discussie en zegt meer over de schrijver van de reactie dan over het stuk. Onthoud dat dit soort reacties ook in Google naar boven kunnen komen
- Social media hebben soms als gevolg dat er een grijs gebied ontstaat tussen privé en werk gerelateerde zaken. Wanneer je op een persoonlijke blog over je werk schrijft, kun je een disclaimer opnemen waarin staat dat dit blog jouw persoonlijke standpunt weergeeft en dat dit niet overeen hoeft te komen met het standpunt van de school

Uit het wetboek van strafrecht:
De grenzen van wat strafbaar is op internet zijn eigenlijk simpel. De wetten en regels die vastgelegd zijn in het wetboek van strafrecht zijn ook online van toepassing. Wat in het echte leven niet mag, mag ook niet online.

Strafbare feiten:

- Belediging (art. 266 en 271)
- Belaging (Stalking art. 285b)
- Bedreiging (art. 285)
- Discriminatie (art. 137d)
- Grooming (art. 248a)
- Hacken (art. 138ab)
- Identiteitsmisbruik (art. 225, 232 en 326)
- Laster / Smaad (art. 261, 262, 268)
- Oplichting (art. 326)
- Uitlokken minderjarige ontuchtige handelingen (art. 248e)