provincie Oost-Vlaanderen

1706003

departement Interne Organisatie
---

dossiernummer: 1706003

Provincieraadsbesluit

betreft **Informatieveiligheid**
ICT-code
verslaggever Martine Verhoeve

1. Feitelijke en juridische gronden

Artikel 42 van het provinciedecreet

De wet van 8 december 1992 betreffende de bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens en haar uitvoeringsbesluiten.

Het decreet van 18 juli betreffende elektronisch bestuurlijk gegevensverkeer en zijn uitvoeringsbesluiten.

2. Motivering

De goede werking van de organisatie is sterk afhankelijk van de vlotte en doeltreffende werking van de Dienst Informatie en Communicatie Technologie (Dienst ICT) en de manier waarop personeelsleden omgaan met ICT middelen. Daarom worden naast de algemene afspraken die in de deontologische code zijn opgenomen, ook afspraken gemaakt vanuit welke waarden en normen het personeel omgaat met ICT en welk gedrag daaraan voldoet.
Deze code voor ICT biedt een algemeen kader met waarden en principes die de personeelsleden van de organisatie, mandatarissen en externen die toegang hebben tot de elektronische communicatiemiddelen van de provincie, moeten respecteren bij het dagelijks gebruik van ICT. Hoewel ICT meestal in verband wordt gebracht met technische aspecten, brengt deze code vooral de sociale en morele aspecten van ICT onder de aandacht.

3. Besluit

Enig artikel.

De provincieraad hecht zijn goedkeuring aan de ICT-code met de hiernavolgende inhoud.

./...

1. Inleiding

1.1. Waarom deze ICT-code?

De goede werking van de organisatie is sterk afhankelijk van de vlotte en doeltreffende werking van de Dienst Informatie en Communicatie Technologie (Dienst ICT) en de manier waarop personeelsleden ermee omgaan. Daarom worden naast de algemene afspraken die in de deontologische code zijn opgenomen, ook afspraken gemaakt vanuit welke waarden en normen het personeel omgaat met ICT en welk gedrag daaraan voldoet.
Deze code voor ICT biedt een algemeen kader met waarden en principes die de personeelsleden van de organisatie moeten respecteren bij het dagelijks gebruik van ICT. Hoewel de meeste mensen ICT dadelijk in verband brengen met technische aspecten, brengt deze code vooral de sociale en morele aspecten van ICT onder de aandacht.

Deze code is ontstaan naar aanleiding van volgende behoeften:

- Een zorgvuldig en duurzaam beheer van ICT-middelen: naast het zorgvuldig en vooruitziend hanteren van ICT-middelen is een duurzaam beheer van deze middelen van groot belang. Bij het omgaan met ICT-middelen speelt de leidinggevende een belangrijke voorbeeldrol. Een degelijk beheer van ICT-middelen blijft niet binnen de grenzen van de werkomgeving, maar geldt ook bij het plaats onafhankelijk werken (zie hoofdstuk 2).
- Het belang van het beveiligen en beschermen van bedrijfsinformatie en persoonsgegevens die niet vallen onder de openbaarheid van bestuur. De beveiliging van ICT-middelen tegen virussen en internetcriminaliteit is ook een belangrijk aandachtspunt (zie hoofdstuk 3).
- De behoefte aan een etiquette voor respectvol communiceren: de kern van de etiquette bestaat erin dat rekening wordt gehouden met de gevoelens van anderen en met de gebruiken in een organisatie, in alle situaties waarin mensen met elkaar omgaan. Door sociale media ontdekken personeelsleden nieuwe mogelijkheden en toepassingen van communiceren, maar dat houdt ook nieuwe risico's in (zie hoofdstuk 4).
- Preventie van misbruik en controle van gebruik van ICT: de maatregelen op dat vlak vloeien voort uit de teksten en aanbevelingen van de Privacycommissie met betrekking tot cybersurveillance (zie hoofdstukken 5 en 6).

1.2. Voor wie is de ICT-code bestemd?

De code geldt voor alle personeelsleden, mandatarissen en externen die toegang hebben tot de elektronische communicatiemiddelen van de provincie. Met externen wordt eenieder bedoeld die geen personeelslid is van de provincie Oost-Vlaanderen (of in die hoedanigheid werkt), of geen gedeputeerde en/of raadslid van diezelfde provincie. Te denken valt aan bv. stagiaires, medewerkers van APB's, VZW's, ingehuurde (project) medewerkers voor zover eea. niet gedekt wordt door contractuele bepalingen.

1.3. Wat zijn ICT-middelen?

./...

De provincie biedt haar personeelsleden en bepaalde werknemers van andere organisaties die bij de provincie een opdracht uitvoeren een aantal informatie-, communicatie- en technologiemiddelen voor de uitoefening van hun taken.
De ICT-middelen kunnen opgesplitst worden in:
- ICT-systemen (hardware en software);
- Informatie op ICT-systemen.

Hardware en software zijn bijvoorbeeld:
- e-mail en internetfaciliteiten;
- programmatuur en applicaties;
- computers, laptops, tablets;
- printers;
- USB-sticks;
- telefoons, gsm's, smartphones;
- opslagmedia (bijvoorbeeld op een server), …

De informatie op de ICT-systemen behoort ook tot de ICT-middelen. De afspraken over het beheer van die informatie vind je in het hoofdstuk over Veiligheid (zie punt 3.4).

2. Hoe omgaan met ICT-middelen?

2.1. Zorgvuldig beheer van ICT-middelen

Met de ICT-middelen die gebruikt worden tijdens het werk ga je om als een **goede huisvader**. Dat principe houdt in dat je je gedraagt als een **vooruitziend en zorgvuldig** persoon.
- '**Vooruitziend**' betekent dat je de nadelige gevolgen van je handelen redelijk probeert in te schatten, dat je er met andere woorden op probeert te anticiperen.
- '**Zorgvuldig**' houdt in dat je die nadelige gevolgen probeert te voorkomen door gepaste voorzorgsmaatregelen te nemen.

Daarnaast ben je bereid **verantwoording** af te leggen over het gebruik van ICT-middelen. De middelen dienen om het algemeen belang na te streven, dus je gebruikt de middelen met het oog op zuinigheid, efficiëntie en effectiviteit.
Hier gelden de specifieke afspraken voor het omgaan met ICT-instrumenten vanuit de deontologische code:
- Gebruik ICT-middelen in overeenstemming met de doelstellingen.
- De meeste softwareproducten zijn gelicentieerd. Voor het installeren van nieuwe software, neem je contact op de datacoördinator van je dienst, of met de ICT servicedesk. Ook heb je soms te maken met auteursrechten (zie punt 4.6) en de privacy. Houd je aan de wettelijke voorschriften.
- Ga kostenbewust om met ICT-middelen. Voor toestellen zoals gsm's, tablets en smartphones hou je je aan de gemaakte afspraken bij je dienst.
- Blijf beleefd en professioneel in je online communicatie, voer geen verhitte discussies en pas op met cynisme en sarcasme. Geschreven berichten komen soms anders over dan bedoeld. Uiteraard houd je je afzijdig van discriminatie, pesten, stalking, spamming, …
- Beveilig de informatie die je zelf door middel van ICT gebruikt en deel de informatie met anderen volgens de afspraken die gelden in je dienst. Neem niet deel aan activiteiten die de beveiliging van de informatie kan schaden, zoals het versturen van kettingbrieven, virussen, valse virusmeldingen, spamberichten. Wees voorzichtig met het openen van bijlagen. Bij vermoeden

./...

van spamberichten, phishing (berichten met doel onrechtmatig informatie te verkrijgen) waarschuw dan de ICT servicedesk.
- Spring zorgvuldig om met je wachtwoorden (zie punt 3.2).

2.2. Voorbeeldrol leidinggevende

Als leidinggevende heb je een **faciliterende rol en een voorbeeldrol** op het vlak van het gebruik van ICT.
- Je denkt zorgvuldig na over de meest gepaste ICT-middelen en over de toegangspolitiek tot systemen die in je dienst wordt gevoerd.
- Je zorgt ervoor dat je personeelsleden de geschikte vorming volgen om de ICT-systemen op een passende manier te gebruiken.
- Je bespreekt mogelijke risico's van het gebruik van ICT met je personeelsleden.
- Je hebt de verantwoordelijkheid om problemen rond ICT-gebruik aan te pakken of aan te kaarten.

2.3. Telewerken / tijds- en plaats onafhankelijk werken

Door de toename van het tijds- en plaats onafhankelijk werken en de moderne informaticamogelijkheden zijn de grenzen tussen privé en werk vaak minder duidelijk. Als je documenten en materiaal mee op verplaatsing neemt (bv. naar huis), tref je de nodige maatregelen om die informatie te beschermen, zowel thuis als onderweg. Op het intranet vind je meer informatie m.b.t. telewerken. Respecteer de bestaande afspraken in de organisatie zoals de in telewerkovereenkomst, en de afspraken binnen je dienst.
Wees terughoudend met het gebruik van privé apparatuur voor werk gerelateerde zaken: de privé apparatuur is (mogelijk) minder beschermd dan uw werk apparatuur. Gevoelige informatie hoort niet thuis op privé apparatuur.

3. Veiligheid

3.1. ICT-veiligheidsbeleid

Als je je laptop, tablet of smartphone **verliest** of deze wordt **gestolen**, moet je dat onmiddellijk aan je leidinggevende en de ICT servicedesk melden. Deze zullen dan het nodige doen (in de mate van het mogelijke) om te voorkomen dat iemand op onterechte wijze toegang verkrijgt tot de werkomgeving van de provincie.

Eenzelfde procedure is van toepassing in de onderstaande gevallen:
- je wachtwoord is gecompromitteerd;
- er staat een virus op je computer;
- je bent het slachtoffer geworden van internetfraude (phishing).

In deze gevallen is het ook nuttig om meteen je computer uit te schakelen of uit het netwerk weg te halen(door de netwerkkabel uit te trekken of wifi uit te schakelen).

In geval van verlies of diefstal dien je bijkomend ook een aangifte te doen bij de politie. Let op dat je steeds passende maatregelen neemt om je ICT-hardware (bv. laptops, notebooks en tablets) te beveiligen: waar mogelijk laat je je apparatuur achter in een afgesloten ruimte/berging, of neem je deze mee naar huis.
In onderstaande gevallen is de apparatuur namelijk niet verzekerd:

./...

- verdwenen (verlies of diefstal zonder sporen van braak, inbraak of diefstal op persoon)
- gestolen, en
  - o geen aangifte bij de politie binnen de 24 uur na het ogenblik van de vaststelling
  - o uit een onvergrendeld voertuig
  - o uit een onbewaakt voertuig tussen 22 uur en 5 uur op openbare weg, openbaar terrein of gemeenschappelijke parking (ook al is de auto vergrendeld).

Het mag duidelijk zijn dat bij verlies of diefstal ook de gegevens op de laptop, tablet of smartphone verloren gaan, en mogelijk in verkeerde handen komen: wees je bewust van de risico's, en zorg dat gevoelige gegevens geëncrypteerd zijn.

3.2. Zorgvuldig omspringen met wachtwoorden

Gebruikers zijn **persoonlijk aansprakelijk** voor alle handelingen die worden uitgevoerd met hun eigen gebruikersidentificatie/wachtwoord.
Deel daarom nooit een wachtwoord mee aan anderen (lijnmanagement, collega's, …) en scherm het wachtwoord af van onrechtmatig gebruik: **wachtwoorden zijn persoonlijk en vertrouwelijk**. Log dus ook niet aan met het account van je collega's (voor het verzekeren van de continuïteit van de dienstverlening wordt geadviseerd om veilige oplossingen te gebruiken zoals bijvoorbeeld het werken met een beveiligde gedeelde schijf, of dienst-postbussen). Schrijf een wachtwoord ook nooit op.

Elk personeelslid is verantwoordelijk voor veiligheid, en het lijnmanagement heeft bovendien een voorbeeldrol. **Het lijnmanagement en de ICT-dienstverlening zullen dus niet vragen naar de wachtwoorden van de medewerkers**.
Gebruik een **sterk wachtwoord**. Een sterk wachtwoord is een wachtwoord dat moeilijk te raden is, maar makkelijk te onthouden, en zo lang mogelijk is. Bij voorkeur gebruikt je een zin.
De volgende regels worden afgedwongen:
- Het wachtwoord bevat minstens 5 tekens;
- Het wachtwoord dient elke 6 maanden veranderd te worden;
- De 5 voorgaande wachtwoorden kunnen niet hergebruikt worden;
- Na 5 keer ingeven van een foutief wachtwoord wordt de gebruikersnaam een half uur geblokkeerd.

3.3. Malware (virussen) en internetcriminaliteit

Malware is de verzamelnaam voor alle 'kwaadaardige software' ('malicious software') zoals virussen, spyware, enzovoort. De mogelijke doelen van malware zijn:

- Informatie te stelen (van de gebruiker of diens systeem);
- De werking van de systemen te ontregelen door gegevens/programma's te verminken of versleutelen;
- Het geïnfecteerde systeem als aanvalswapen in te zetten richting andere systemen.

De verspreiding van malware gebeurt nog vaak via e-mail, ofwel als bijlage ofwel als link naar iets wat je kunt downloaden met de browser, zoals een

./...

'gratis' programma. Het is mede daarom dat de gebruiker niet zelf (niet gekende) programmatuur kan installeren.
De bedreiging van **internetcriminaliteit** bestaat in vele vormen en neemt steeds toe. Het is belangrijk waakzaam te zijn tegen gerichte aanvallen zoals internetfraude of phishing, een vorm van oplichting waarbij men hengelt naar persoonlijke informatie zoals bv. creditcardnummer, wachtwoord en accountgegevens. Soms nemen criminelen ook persoonlijk contact op met de gebruiker, per e-mail of per telefoon, en proberen ze de gebruiker over te halen om bepaalde handelingen uit te voeren ('social engineering').
Hieronder vind je adviezen om te voorkomen dat je het slachtoffer wordt van internetcriminaliteit.

- Laat de veiligheidsmaatregelen op je computer intact (firewall, antivirus software enzovoort).
- Vertrouw nooit blindelings afzendergegevens in e-mailberichten.
- Denk na over de context van het bericht: 'Klopt het dat ik dit bericht ontvang van deze persoon of organisatie?'.
- Open geen verdachte e-mails en beantwoord ze vooral niet. Open zeker niet de bijlage en bezoek ook niet de links die erin staan. Bij twijfel, kun je het best (telefonisch) contact opnemen met de afzender van het bericht.
- Wees alert als iemand die je niet kent contact met je opneemt (per e-mail of per telefoon). Geloof niet zomaar alles wat men je vertelt en wees op je hoede als men je probeert over te halen om een handeling uit te voeren.
- Vermoed dat je computer door malware is getroffen of dat men je heeft proberen te benaderen als onderdeel van een aanval, neem dan onmiddellijk contact op met de ICT servicedesk.

3.4. Beheer van informatie

3.4.1. Openbaarheid van bestuur versus vertrouwelijke informatie

De organisatie beschikt over een grote hoeveelheid aan informatie. Veel van die informatie stellen we ter beschikking van de burger in het kader van de openbaarheid van bestuur.
Daarnaast is een groot deel van de informatie **vertrouwelijk**, omdat de belangen van de betrokkenen worden geschaad bij openbaarmaking van de informatie:
- belangen van natuurlijke personen, bijvoorbeeld gegevens die onder het medische geheim vallen, tuchtdossiers, dossiers met persoonsinformatie; gegevens van burgers;
- belangen van de organisatie, bijvoorbeeld het geheim van beraadslagingen van organisaties die politieke beslissingen nemen, informatie over een interne audit;
- belangen binnen gerechtelijke procedures, bijvoorbeeld informatie m.b.t. gerechtelijke procedures of strafrechtelijke feiten waarbij de organisatie betrokken partij is;
- zaken van maatschappelijk belang, bijvoorbeeld informatie die invloed kan hebben op de openbare orde en veiligheid of informatie die een economisch, financieel of commercieel belang kan schaden.

Je denkt na over het soort van informatie waarover je beschikt en je verspreidt de informatie alleen als je er zeker van bent dat het niet over vertrouwelijke gegevens gaat. Bij twijfel neemt je steeds contact op met je leidinggevende.

./...

De verspreiding of verwerking van bepaalde persoonsgegevens mag enkel met een aangifte of een machtiging van de Privacycommissie (www.privacycommission.be/nl).
Transport van vertrouwelijke gegevens (door bijvoorbeeld je laptop of een USB-stick mee te nemen) beperk je tot situaties waarin dat strikt noodzakelijk is voor de uitvoering van je werk. Je bent je in een dergelijke situatie steeds bewust van de risico's en versleutelt de gegevens.

3.4.2. Verantwoordelijkheid beheer van informatie

Voor een papieren document is het vaak gemakkelijk om zelf de vertrouwelijkheid te garanderen. Je kunt het document zelf op **een veilige plaats** wegbergen. Voor elektronische bestanden geldt er een **gedeelde verantwoordelijkheid** tussen de beheerders van de ICT-opslagmogelijkheden en jezelf.
- De beheerders garanderen dat onbevoegden geen toegang hebben tot de systemen door het gebruik van firewalls, door een wachtwoordenbeleid, en toegangsbeheer.
- Je bent zelf verantwoordelijk voor de juiste en meest veilige opslag van je bestanden en voor je eigen wachtwoord. Dat wil zeggen dat je:
    - werkgerelateerde bestanden opslaat in het gemeenschappelijk klassement op de juiste plaats. Zo kun je informatie delen met je collega's en is er geen verlies van informatie mogelijk, aangezien van alles een back-up wordt gemaakt. Het is niet de bedoeling om in documenten te gaan snuffelen waar je niets mee te maken heeft ook al zou dat mogelijk zijn;
    - je computer vergrendelt telkens als je je computer alleen laat, of uitschakelt indien je langere tijd (meer dan een uur) afwezig zult zijn.

Een gedeelde verantwoordelijkheid geldt als er een contract is met de beheerders. Een contract op maat is vaak niet mogelijk bij **cloud-toepassingen**. Cloud-computing is ICT dienstverlening via het internet, bijvoorbeeld het aanbieden van (gratis) opslag of programmatuur.
Als je informatie op een cloud platform zet (zoals bv. LinkedIn, Facebook, Dropbox, Google Docs, WeTransfer, …) dan bent je onderworpen aan de voorwaarden van dat platform. Dat je bedrijfsinformatie op een cloud-toepassing zet waar ze is afgeschermd met een login en wachtwoord, betekent nog niet noodzakelijk dat die informatie daar veilig staat. Dit is zeker het geval voor Amerikaanse cloud aanbieders, omdat Amerikaanse wetgeving toestaat dat deze gegevens ingezien mogen worden.

Bij cloud-toepassingen gelden de volgende afspraken:
- Weeg goed af of het nodig is of een meerwaarde heeft om data op te slaan op het desbetreffend cloud-platform. Een applicatie die door de eigen organisatie wordt aangeboden, verdient steeds voorkeur.
- Sla alleen niet-vertrouwelijke en niet-kritische data voor de organisatie op in de cloud-toepassing, gelet op de beperkte zekerheid rond beveiliging. Bij voorkeur wordt deze data geëncrypteerd. Sla zeker geen privacygevoelige gegevens op.
- Zorg ervoor dat je het overzicht behoudt over welke informatie waar staat.
- Vertrouw niet alleen op een cloud-platform voor de beschikbaarheid van data (cloud-diensten komen en gaan, passen hun voorwaarden en financiering of kostprijs aan en zijn meestal niet aansprakelijk als de dienst een paar uur of enkele dagen niet beschikbaar is).

./...

3.4.3. Opslag van informatie

Over de **opslag van informatie** gelden de volgende afspraken:
- Sla geen bestanden op met commercieel karakter of voor privé-nevenwerkzaamheden.
- Persoonlijke bestanden kunnen onder de map C:\privé opgeslagen worden.
- Bewaar geen bestanden die:
    - obsceen of beledigend zijn;
    - in strijd zijn met de openbare orde;
    - n strijd zijn met de goede zeden;
    - het privéleven van iemand aantasten;
    - discriminerend, racistisch, seksistische of xenofobisch zijn of die tot een dergelijk gedrag aanzetten;
    - onwettige informatie bevatten, zoals hacking software;
    - een inbreuk zijn op de auteursrechten, zoals bij muziekbestanden, films, software die je op een illegale manier verkregen hebt.

Het illegaal downloaden van bestanden is niet toegestaan. Je mag dergelijke bestanden ook niet opslaan of verder verspreiden.

4. Communicatie

4.1. Hoe communiceren?

Als basisregel geldt '**respectvol communiceren**', zowel bij interne als externe communicatie.
In deze rubriek vind je meer informatie over wat dat concreet betekent voor het communiceren met:
- telecommunicatie;
- e-mail;
- internet en intranet;
- sociale media.

Daarbij respecteer je de auteursrechten (*zie punt 4.6*).
Indien je twijfelt kun je steeds advies vragen bij de dienst communicatie, zij helpen je graag verder.

4.2. Behoorlijk telecommunicatie gebruik

Onder telecommunicatiegebruik valt het gebruik van gsm, smartphone, telefoon, fax, enzovoort. Hoewel het gebruik van andere communicatiemiddelen (bijvoorbeeld e-mail, internet) groeit binnen de samenleving, blijft de telefoon een belangrijk contactmiddel. Een **goede bereikbaarheid en een correcte dienstverlening** blijven dan ook noodzakelijk.

4.3. Behoorlijk e-mailgebruik

./...

E-mail is een **populair, effectief en efficiënt** communicatiemiddel binnen de organisatie met onmiskenbare voor- en nadelen. Het volgen van onderstaande richtlijnen garandeert dat e-mail een goed hulpmiddel is en blijft voor ons werk.

4.3.1. Gebruik en het beheer van e-mail

Hieronder vind je een aantal adviezen voor een efficiënt gebruik van e-mail:
- Geef steeds een duidelijke omschrijving in de onderwerpregel van het e-mailbericht. De onderwerpregel vat je bericht samen zoals een krantenkop.
- Wees zuinig met cc. Stuur het bericht uitsluitend naar personen die echt op de hoogte moeten zijn of die expliciet om een kopie van het bericht hebben gevraagd.
- Vermijd het gebruik van 'allen beantwoorden'. Vaak is het niet nodig dat alle geadresseerden bij de zaak worden betrokken. Stuur je antwoord of bedenkingen alleen terug naar hen voor wie dit direct relevant is.
- Met de mailbox-functie 'prioriteit hoog' laat je de lezer van je e-mail weten dat die e-mail dringend behandeld moet worden. Gebruik de functie daarom alleen voor dringende berichten.
- Verkies persoonlijk contact boven e-mail. Zeker als de collega voor wie je een vraag hebt dichtbij zit, kun je hem of haar beter rechtstreeks aanspreken.
- Gebruik e-mail nooit voor één op één gesprekken, discussies, meningsverschillen of emotioneel geladen boodschappen. Gebruik de telefoon voor dringende of complexe vragen.
- Beperk de bijlagen zowel wat het aantal als de grootte ervan betreft, en definieer steeds duidelijk hun inhoud.

Hieronder vind je enkele afspraken voor het beheer van **dienst-mailadressen**. Er bestaan immers heel wat dergelijke dienst postbussen die e-mails versturen én ontvangen.
- Bij het aanmaken van dienst postbussen moet er grondig worden nagegaan of het zinvol is een generiek adres te creëren.
- Een dienst postbus wordt minstens elke dag eenmaal geopend. Als dat nodig is, wordt de postbus frequenter geopend.
- Alle e-mails worden beantwoord, ofwel meteen, ofwel met een boodschap dat de vraag werd ontvangen en wordt behandeld door de persoon in cc. Mensen beschouwen e-mail als een snel medium, dus verwachten ze een snelle reactie.
- E-mails vanuit een dienst postbus worden nooit anoniem verstuurd, maar uit naam van de behandelend ambtenaar. Indien je ook een telefoonnummer meegeeft, bij voorkeur het algemene nummer van een teamsecretariaat of afdeling.

Personeelsleden gebruiken soms een privé-account voor persoonlijke e-mails (bijvoorbeeld via Hotmail, Gmail, Telenet, …) om werk en privémailverkeer van elkaar te scheiden. Let hierbij op: je persoonlijke mail-account wordt niet door de systemen van de provincie gescand – het gevaar is dat je op die manier de systemen compromitteert.
Het is eerder aangeraden om alle verzonden en ontvangen persoonlijke e-mails te bewaren in een aparte map, waarvan de naam begint met 'Privé', bij voorkeur aangevuld met de naam van de betrokken werknemer. Als medewerkers persoonlijke e-mails versturen via het werkmailadres, zijn die e-mails onderworpen aan de gangbare controles (*zie hoofdstuk 6*). Deze aanbeveling is een preventiemiddel om controles en het opsporen van

./...

misbruiken te vermijden en de schending van het privéleven van de medewerker zoveel mogelijk te beperken bij die controles.

4.3.2. Inhoud van e-mail

Over de inhoud van de e-mails gelden volgende afspraken:
- Pas eerst en vooral tijdens de uitoefening van je functie dezelfde basisprincipes toe voor e-mailberichten als bij de gewone briefwisseling of bij een telefoongesprek: communiceer correct en vermeld je naam en contactgegevens.
- Gebruik enkel je eigen login en wachtwoord om e-mails te verzenden.
- Gebruik geen andere handtekening dan de uwe.
- Verstuur neutrale berichten, dus geen berichten met een commercieel, politiek en/of religieus karakter.
- Verstuur geen berichten die:
    - obsceen of beledigend zijn;
    - in strijd zijn met de openbare orde;
    - in strijd zijn met de goede zeden;
    - het privéleven van iemand aantasten;
    - discriminerend of xenofobisch zijn of tot een dergelijk gedrag aanzetten;
    - onjuiste informatie (zoals kettingbrieven) of malware bevatten, indien je een dergelijke mail ontvangt contacteer je de ICT-servicedesk.
- Houd er rekening mee dat een e-mail zich niet zo goed leent voor vertrouwelijke communicatie. Een kleine fout kan ervoor zorgen dat een bericht ongewenst bij de verkeerde personen terechtkomt. Zet geadresseerden die elkaars gegevens niet mogen kennen in bcc.
- Respecteer de auteursrechten (*zie punt 4.6*).
- Houd het kort. E-mail is bedoeld voor snelle informatie-uitwisseling, begin daarom je e-mail meteen met de conclusie of actie.
- Ruim regelmatig je mailbox op door oude of overbodige berichten te verwijderen. Die zorgen voor een onnodige belasting van de opslagschijven op de servers. Maak de map ‘verwijderde items’ regelmatig leeg.
- Stuur geen e-mails automatisch door naar een eigen externe mailbox (bijvoorbeeld Hotmail, Gmail, Telenet, …). De veiligheid van de berichten bij die aanbieders kan immers niet gegarandeerd worden.
- Maak gebruik van afwezigheidsberichten. Geef daarin aan vanaf wanneer mails niet meer en weer wel worden gelezen en bij wie de correspondent in de tussentijd terecht kan (eventueel voor welke thema’s) en vermeld de contactgegevens van die persoon, personen of dienst e-mailadres.

4.3.3. E-mail filtering

De organisatie filtert het (officiële) e-mailverkeer op virussen en spam, en hoewel dit het risico van spam-mail en/of virussen vermindert, blijft de mogelijkheid aanwezig.

4.4. Behoorlijk intranet- en internetgebruik

De meeste collega’s hebben toegang tot het intranet en het internet. Dat biedt de mogelijkheid om veel nuttige informatie voor het werk op te zoeken.

./...

De organisatie verwacht van haar medewerkers de discipline en verantwoordelijkheid om het internet correct en efficiënt als werkinstrument te gebruiken. Luisteren naar de radio of tv-kijken met live-streaming neemt bijvoorbeeld veel bandbreedte in. Dat vertraagt het netwerk en heeft dus gevolgen voor het werk van collega's. Zorg daarom voor een redelijk, professioneel en zinvol gebruik van het internet tijdens het werk (*zie ook punt 4.5*).
Bij de organisatie is **beperkt privégebruik** van het internet toegestaan onder bepaalde voorwaarden:
- voor zover het is toegestaan binnen de eigen dienst;
- als het de uitvoering van je taken en je productiviteit en die van je collega's niet in het gedrang brengt.

Het is echter niet toegestaan om bepaalde sites te bezoeken en bestanden voor privédoeleinden te downloaden.
Sites die niet kunnen:
- sites die zich tegen de grondbeginselen van de democratie en de rechtstaat keren, zoals sites die in verband staan met racisme, terrorisme, discriminatie, …;
- sites die anderen kunnen kwetsen of beledigen, zoals sites met racistische of seksistische onderwerpen, pornografisch materiaal, schokkende foto's, …;
- sites die een gevaar voor verslaving vormen zoals goksites en pornografische sites.

Als preventiemiddel kan de **toegang tot bepaalde internetsites geblokkeerd worden** (*zie hoofdstuk 5*). De organisatie verwacht immers van haar werknemers dat ze internet als werkinstrument gebruiken. Ook kan het veelvuldig bezoeken van bepaalde sites het netwerk belasten.
In sommige situaties kunt je zelf informatie op internet of intranet plaatsen. Als je die middelen gebruikt om zelf te communiceren, volg dan de algemene richtlijnen die van toepassing zijn op overheidscommunicatie en de regels rond spreekrecht, spreekplicht en zwijgplicht uit de deontologische code.
Daarnaast respecteer je de auteursrechten (*zie punt 4.6*).

4.5. Sociale media

Bij de organisatie wordt een brede definitie van sociale media gehanteerd. Het gaat om interactieve internettoepassingen die een multimediale dialoog tussen gebruikers van het medium mogelijk maken. Cruciaal daarbij is dat de gebruiker niet alleen consumeert, maar ook gemakkelijk zelf inhoud aan het medium kan toevoegen. Het gaat dus om tweerichtingsverkeer.
Veel personeelsleden van de organisatie gebruiken sociale media en dat geeft heel veel mogelijkheden:
- je kunt er kennis mee delen;
- je kunt je professionele ideeën toetsen aan de realiteit;
- je kunt in contact komen met andere medewerkers, experts in je vakgebied, burgers, enzovoort.

Tegelijk brengt dat ook een paar **risico's** mee: hoe scheid je werk en privé? Als personeelslid van de Provincie Oost-Vlaanderen vertegenwoordig je onze organisatie bij élk contact met iemand van buitenaf, of dat nu beroepsmatig of privé is. Zo bepaal je in grote mate het imago van ons bestuur. In alles wat je zegt of schrijft, ben je een ambassadeur van de Provincie. De richtlijnen voor het gebruik van sociale media bieden een houvast voor je aanwezigheid op het

./...

internet. [ter info: de richtlijnen sluiten aan bij de strategie voor het invoeren van sociale media, zoals goedgekeurd door deputatie op 9/2/2012]

4.6. Auteursrechten

4.6.1. Gebruik van materiaal en informatie door een werknemer

Voor het gebruik van materiaal en informatie gelden de bepalingen van het Wetboek van economisch recht zoals toegevoegd door de wet van 19 april 2014 (“Wet houdende invoeging van boek XI, "Intellectuele eigendom" in het Wetboek van economisch recht, en houdende invoeging van bepalingen eigen aan boek XI in de boeken I, XV en XVII van hetzelfde Wetboek”). Dat betekent onder meer dat je alleen teksten of afbeeldingen van derden mag verspreiden en gebruiken met de **toestemming van de oorspronkelijke auteur**.
Wees zorgvuldig bij het publiceren van informatie en publiceer geen onwettige informatie of informatie die schade kan berokkenen aan derden.

4.6.2. Productie van materiaal/informatie door de werknemer

Personeelsleden dragen in principe alle **vermogensrechten aan de organisatie** over op de werken die bij de uitoefening van hun functie tot stand zijn gebracht en waarvan ze de (mede)auteur zijn.
Dat wil zeggen dat de auteursrechten op werken die niet bij de uitoefening van het ambt tot stand worden gebracht in principe aan het personeelslid blijven toebehoren.

5. Preventiemiddelen

De leidinggevenden treden eerst en vooral preventief op om:
- controles te *vermijden*;
- het opsporen van misbruiken te *vermijden*;
- bij eventuele controles de privacy zoveel mogelijk te respecteren.

De volgende preventieve maatregelen kunnen genomen worden:
- De toegang tot bepaalde sites kan geblokkeerd worden. De organisatie verwacht immers van haar werknemers dat ze internet als werkinstrument gebruiken. Het veelvuldig bezoeken van bepaalde sites kan bovendien het netwerk belasten.
- Alle werkgerelateerde informatie wordt bij voorkeur bewaard op media die toegankelijk zijn voor de leidinggevenden en collega’s (en systeembeheer). Persoonlijke bestanden op die opslagmedia worden duidelijk als ‘privé’ aangeduid.
- Bij een geplande langdurige afwezigheid worden afspraken gemaakt over:
    - het doorsturen van e-mails;
    - het plaatsen van afwezigheidsboodschappen in e-mailaccounts;
    - het plaatsen van werkgerelateerde bestanden op opslagmedia die door verschillende medewerkers worden gedeeld.

- Bij een onverwachte en mogelijke langdurige afwezigheid van een medewerker wordt er zo snel mogelijk gezorgd voor een

./...

afwezigheidsboodschap (waar dit niet meer mogelijk is door de medewerker zelf zal dit via de ICT-servicedesk gedaan worden). Zo zijn alle correspondenten van het afwezige personeelslid op de hoogte van diens afwezigheid en beschikken ze over de contactgegevens van andere medewerkers bij wie ze terecht kunnen.
- Het gebruik van dienst- mailadressen (of dienst-postbussen) kan nuttig zijn om mogelijke afwezigheden, of niet beschikbaar zijn van medewerkers op te vangen.

6. Controlemiddelen

Het bestuur heeft het recht om een controle uit te oefenen op de elektronische on-line communicatie van de medewerkers. Deze controle is niet beperkt tot de eigen medewerkers, maar betreft alle gebruikers van de netwerkdiensten van de provincie. De privacy van de gebruikers dient hierbij zoveel als mogelijk gerespecteerd te worden. De controle moet getoetst worden aan:
- het finaliteitsbeginsel: een controle is alleen mogelijk voor het nastreven van gerechtvaardigde doelen;
- het transparantiebeginsel: er wordt open gecommuniceerd over de controles en de doelen en voorwaarden van de controles;
- het proportionaliteitsbeginsel: de controle en het soort controle moeten in verhouding staan tot het doel van de controle.

Die drie beginselen hebben als doel het evenwicht te houden tussen:
- het recht van de werkgever op controle van werkmiddelen;
- het recht van de werknemer/netwerkgebruiker op zijn privéleven.

In het arbeidsreglement worden in titel 11.2 de controle- en individualiseringsmaatregelen besproken. Een kort overzicht:
De controles kunnen betreffen:
- het gebruik van internet – lijst van geraadpleegde websites (duur en tijdstip bezoek);
- het gebruik van e-mail – algemene gegevens zoals: frequentie, aantal, omvang, bijlagen;

Incidentele gebruikers van de netwerkdiensten (bv. bezoekers) worden in de gebruiksvoorwaarden gewezen op de controlemogelijkheden.
Indien de algemene controles daartoe aanleiding zouden geven kan overgegaan worden tot identificatie van de gebruiker. Dit kan op directe of indirect manier gebeuren:

./...

- Indirect: personeelsleden worden op de hoogte gebracht van de schending van de gedragsregels, bij herhaling binnen de 3 maanden zal het betrokken personeelslid geïdentificeerd en gehoord worden.
- Direct: bij zware inbreuken (schending vertrouwelijkheid, plegen van ongeoorloofde of lasterlijke feiten), zal het betrokken personeelslid geïdentificeerd en gehoord worden. Indien het niet-personeelsleden betreft zullen de controlegegevens overgemaakt worden aan de bevoegde instanties.

Waar het personeelsleden betreft zullen passende sancties genomen worden.

Gent, 13 december 2017

namens de Provincieraad:

De provinciegriffier,
Albert De Smet

De voorzitter,
Greet De Troyer