# rechtspositieregeling-arbeidsreglement
# bijlage 2
# code voor het gebruik van informatica- en communicatiemiddelen

## Inleiding

De ict-infrastructuur (vaste en mobiele telefoons, vaste computers, laptops, e-mail, intranet, internet, wifi, printers, faxen en kopieermachines) zijn middelen die het bestuur als werkgever aanbiedt aan haar personeelsleden om hun taken efficiënt en naar behoren uit te voeren. Het bestuur is er immers van overtuigd dat deze moderne communicatiemiddelen de kwaliteit van de arbeid en de dienstverlening verhogen.

Het is belangrijk dat er duidelijke richtlijnen zijn over het gebruik ervan opdat u, als gebruiker, weet wat aanvaardbaar gebruik is. Elke medewerker is verantwoordelijk voor haar of zijn communicatiegedrag.

Deze gedragscode is gebaseerd op de wetgeving ter zake en is bedoeld om de ict-infrastructuur optimaal te laten functioneren voor alle gebruikers.

## Doel van de afspraken

De gedragscode bevat aanbevelingen en adviezen over het correct gebruik van de ict-infrastructuur, het gebruik van het netwerk en het gebruik van het internet (e-mail, surfen,…). We verlangen van elke medewerker dat hij voor zijn communicatie gebruik maakt van het gepaste medium.

Deze gedragscode bevat ook mededelingen over de wijze waarop het bestuur omgaat met het registreren, verzamelen en monitoren van tot een persoon herleidbare gegevens over het e-mail-, internet-, en telefoongebruik.

Tenslotte wordt gewezen op mogelijke sancties die bij eventuele misbruiken getroffen kunnen worden.

Naast deze gedragscode werd eveneens een afsprakennota opgemaakt, specifiek rond het gebruik van mobiele telefoons.

## 1. Gebruik van telefoon, gsm en smartphone

Deze paragraaf geldt tot wanneer er een nieuwe afsprakennota rond het gebruik van mobiele telefonie beschikbaar komt.

### *Doelgroep*

Iedereen die gebruik maakt van een telefoon of smartphone van het bestuur.

### *Algemeen uitgangspunt*

In principe wordt de telefoon enkel gebruikt voor de uitvoering van uw taak. Probeer het gebruik van de telefoon voor privégesprekken zoveel mogelijk te vermijden.

Gebruik de telefoon voor dringende berichten en/of als de bestemmeling beschikbaar is.

### *Controle*

Bepaalde gegevens inzake telecommunicatie worden verzameld en kunnen gecontroleerd worden. Onder bepaalde gegevens verstaan we: een inventaris van de opgeroepen abonneenummers, alsook het type, het tijdstip van aanvang en de duur van de oproepen, evaluatie van gemaakte telefoonkosten,…

Kennisname van de inhoud van telefoongesprekken is niet toegestaan.

## 2. Gebruik van de ict-infrastructuur en van het netwerk

### *Doelgroep*

Iedereen die voor de uitoefening van zijn/haar taak toegang heeft tot het netwerk, na het toekennen van een login door de systeembeheerder, en/of over een telefoon/mobiele telefoon beschikt.

### *Algemene bepalingen*

Het gebruik van de ict-infrastructuur (vaste en mobiele telefoons, computers, e-mail, wifi, intranet, internet, printers, faxen en kopieermachines) inbegrepen het gebruik van het netwerk en het medium internet (e-mailen, surfen,..) is enkel toegestaan voor de uitvoering van de opgelegde taken.

Tijdens de diensturen moeten de personeelsleden zich volledig aan hun job wijden en mogen zij geen ongeoorloofd gebruik maken van de uitrusting of het materiaal van het bestuur voor privédoeleinden.

Ongeoorloofd gebruik is ruimer dan illegaal gebruik en omvat ook het gebruik van e-mail en internet voor private of commerciële doeleinden, of een gebruik dat de infrastructuur kan overbelasten.

Het bestuur erkent dat u bij de uitoefening van uw taak recht hebt op respect voor uw persoonlijke levenssfeer en dat u occasioneel privécontacten mag onderhouden met collega's en met derden buiten het bestuur, maar slechts voor zover dit niet storend is voor uw normale werkzaamheden. Het toezichthoudend personeel of de systeembeheerder kunnen vaststellen wanneer privégebruik zijn occasioneel en beperkt karakter overschrijdt.

In de mate dat privégebruik toegestaan wordt, gaat het om een gunst en niet om een recht, die steeds kan beperkt of ingetrokken worden.

### *Behoud van netwerk en systeemcapaciteiten*

Internetverkeer en internetdiensten op de servers van het bestuur hebben uiteraard invloed op de beschikbare capaciteit (de bandbreedte en de vrije schijfruimte) en op de computerhardware en -software. Behoed ons netwerk voor misbruik en optimaliseer op die manier mee de vlotte werking en antwoordtijden.

Er gebeurt een standaard logging van wie naar welke websites surft, wanneer dat gebeurt en hoe lang dat duurt. Ook de hoeveelheid of het type van gedownloade bestanden wordt geregistreerd.

### *Paswoord*

Het gebruik van een uniek paswoord voor aanmelding op het netwerk is verplicht. Het paswoord bepaalt uw rechten op het netwerk. Maak gebruik van een paswoord dat minstens 8 karakters lang is, dat grote en kleine letters bevat, en minstens een cijfer en een speciaal karakter (& @ # ! …).

U mag niet werken met een login en paswoord van anderen. Het paswoord is strikt persoonlijk en geheim. Geef uw paswoord niet door tenzij aan de systeembeheerder, indien strikt noodzakelijk.

### *Onbeheerd laten van een pc*

Indien u uw computer onbeheerd achterlaat (vergadering, buitendienst, middagpauze,….) moet u uw computer vergrendelen of zich afmelden. Openstaande logins op de toepassingen

moeten na gebruik en zeker tijdens de middagpauze gesloten worden, ter beveiliging tegen gebruik door onbevoegden.

### *Software*

Software mag alleen door de systeembeheerder of in zijn opdracht geïnstalleerd (of gedownload) worden. Indien blijkt dat bepaalde toepassingen op pc's werden geïnstalleerd zonder overleg met de systeembeheerder, kan hij deze programma's verwijderen.

Niet-legale software, spelprogrammaatjes en niet voor de dienst bestemde toepassingen (ook gratis free- of shareware) zijn niet toegelaten. Ook het kopiëren van software van computers van het bestuur is niet toegestaan. Het zijn de gebruikers zelf die juridisch aansprakelijk gesteld worden indien misbruiken vastgesteld worden.

### *Anti malware*

Elke computer is voorzien van anti-malwaresoftware. Deze beschermt uw toestel tegen virussen en andere malafide software. Het is strikt verboden deze software uit te schakelen. Indien de systeembeheerder merkt dat u deze antivirussoftware uitgeschakeld hebt, kan hij u de toegang tot het netwerk onmiddellijk ontzeggen. Gezien het groot belang van het correct gebruik van antivirussoftware voor onze organisatie wordt het gebruik ervan ten allen tijde opgevolgd. Het is niet toegestaan om toestellen op ons netwerk te koppelen, die niet voldoen aan de minimum veiligheidsvereisten die de dienst ict vooropstelt.

### *Gebruik van het netwerk*

Door u aangemaakte bestanden slaat u steeds op de netwerklocaties op en niet op uw eigen harde schijf (C-schijf). Er wordt geen reservekopie gemaakt van bestanden op uw harde schijf. Bij het vervangen van uw pc zal geen rekening worden gehouden met de eventueel aanwezige bestanden op uw lokale harde schijf.

De personeelsleden worden gevraagd zuinig om te springen met de schijfruimte van de bestandsserver. Overbodige bestanden moeten regelmatig verwijderd worden. Niet vaakgebruikte bestanden zullen periodiek op externe of draagbare media (cd, dvd) geplaatst worden in samenspraak met de systeembeheerder.

Alle mededelingen die op het intranet gepubliceerd worden, worden verondersteld door iedereen gelezen te zijn.

### *Beschikbaarheid van de toepassingen en continuïteit van de dienst*

U dient er mee zorg voor te dragen dat er geen toepassingen in gebruik zijn waar niemand anders dan uzelf mee overweg kan. Om problemen in geval van ziekte of vakantie te vermijden, moeten alle toepassingen door minstens twee medewerkers van de dienst gebruikt kunnen worden. Roep desnoods de hulp van de systeembeheerder in om zulke toepassing dubbel te installeren en zorg ervoor dat voldoende collega's de nodige paswoorden van de toepassing kennen. De gegevens van zulke toepassingen moeten op de netwerkserver staan om gebackupt te kunnen worden.

### *Gebruik van externe media, zoals diskettes, usb-toestellen en cd's*

Het gebruik van externe media is toegestaan indien het met de nodige voorzichtigheid gebeurt. Gebruik enkel media die je bekend zijn. Gebruik nooit zomaar CD's of USB-sticks die ergens gevonden werden. Alle media dienen voor elk gebruik (lezen of schrijven) gescand te worden op virussen en malware. Dat geldt ook voor media die u door bekenden ter beschikking worden gesteld. Vraag zo nodig assistentie van de dienst ict.

### *Beheer van uw pc*

Iedereen is persoonlijk mee verantwoordelijk voor de goede werking van zijn computer. In geval van problemen of vreemde fenomenen, dient u deze dadelijk te melden aan de systeembeheerder.

Wanneer u vermoedt dat uw toestel besmet is door malware, of wanneer u vreemde zaken op het scherm te zien krijgt, dan moet u onmiddellijk het toestel loskoppelen van het netwerk, desnoods door de netwerkkabel los te maken. Eventueel trekt u gewoon de stroomdraad los. Bij draagbare toestellen kan het nodig zijn om ook de batterij te verwijderen. Zorg dat u op voorhand weet hoe dat moet.

Indien u telefonisch of op een andere manier zou gecontacteerd worden door iemand die niet tot onze organisatie behoort (maar van Microsoft of een of andere helpdesk) en die beweert dat er een probleem is met uw computer, dan moet u die persoon verwijzen naar de dienst ict, er geen gesprek mee aangaan, geen andere contactgegevens doorgeven, en zeker niet op e-mails of links klikken die die persoon u zou bezorgen. Meld dit soort voorvallen altijd onmiddellijk per telefoon (of via ict@westerlo.be ingeval van afwezigheid) aan de dienst ict en aan de verantwoordelijke voor informatieveiligheid.

### *Discretie*

Medewerkers met een loketfunctie moeten voldoende aandacht hebben voor discretie en zo mogelijk hun beeldscherm zodanig opstellen dat het niet leesbaar is voor onbevoegden.

## 3. Internetgebruik

### *Doelgroep*

Iedereen die gebruik maakt van de internettoegang van het bestuur.

### *Algemeen uitgangspunt*

Alle personeelsleden worden aangemoedigd het internet te gebruiken voor het beter uitvoeren van de hen toevertrouwde taken.

Bij het gebruik van de internettoegang moeten de normale deontologische regels van de ambtenaar gerespecteerd worden. Alle elektronische communicaties over zakelijke onderwerpen die verband houden met het bestuur zijn toegestaan. De internetdiensten (het internetsurfen, e-mail, nieuwsgroepen,…) mogen enkel gebruikt worden voor activiteiten in verband met het bestuur, om werkzaamheden uit te voeren die nodig zijn om uw opdrachten te vervullen of voor professionele training of studies.

Tijdens de middagpauze mogen de ambtenaren voor eigen gebruik surfen, mits zij de afspraken over de niet toegestane sites naleven.

### *Niet toegestaan*

Volgend gebruik van internet is niet toegestaan tijdens uw werkuren:

- persoonlijke activiteiten buiten de normale werkactiviteiten van de medewerker
- verkoops- of winstmakende activiteiten alleen te gunste van de medewerker
- het gebruik van nieuwsgroepen is, tenzij het professionele nieuwsgroepen betreft.
- het is verboden om bij de uitvoering van uw arbeid gebruik te maken van private adressen (vb. Hotmail of Gmail). Alle elektronische correspondentie die gebruik maakt van de bestuurlijke internettoegang, dient te verlopen langs het officiële elektronische adres (dienst@westerlo.be; voornaam.familienaam@westerlo.be).

- u mag bij het versturen van elektronische gegevens uw identiteit niet verbergen, tenzij dit omwille van de omstandigheden toch te verantwoorden is (vb. inschrijven in een professionele nieuwsgroep om redenen van beroepsgeheim,…)

Volgend gebruik van internet is nooit toegestaan op ons netwerk:

- het bezoeken van pornosites of sites die geweld of onwettige handelingen aanmoedigen
- het bezoeken van sites die racisme en onverdraagzaamheid uitdragen.
- het beluisteren van radioprogramma's of bekijken van internet-tv.
- downloaden en installeren van programma's, muziek, foto's, films, ... Indien u meent dat er toch een programma's geïnstalleerd moet worden, dan kan dit enkel met medeweten of onder toezicht van de systeembeheerder.
- het opzetten van allerhande chatsessies met onbekenden. De kans op het oplopen van virussen en op inbraak vergroot hierdoor immers sterk.
- het is verboden via de internettoegang van het bestuur binnen te breken in de eigen sites of in ieder ander netwerk of site. U mag op geen enkele wijze tussenkomen in de normale werking van het netwerk, noch van enig ander netwerk, zeker niet met de bedoeling deze werking te verstoren.
- u mag de internettoegang niet gebruiken om op enige wijze de goede naam of reputatie van het bestuur van Westerlo in het gedrang te brengen.
- onwettelijke activiteiten, waaronder het zenden of ontvangen van materiaal waarop auteursrechten bestaan en die dus een inbreuk betekenen op de wetgeving op auteursrechten of licentieovereenkomsten.
- het versturen of ontvangen van seksueel expliciete of aanstootgevende berichten, cartoons, moppen, etnische beledigingen, racistische uitspraken of enige andere inhoud die aanzien zou kunnen worden als een aanval, vernedering of belediging.
- het versturen van vertrouwelijke informatie of gegevens met een privaat karakter, al dan niet eigendom van het bestuur (zoals documenten, software of foto's) aan iemand die niet gerechtigd is hiervan kennis te nemen of deze informatie te ontvangen.

# 4. E-mailgebruik

## *Doelgroep*

Iedereen die over een e-mailaccount (voornaam.familienaam@westerlo.be of dienst@westerlo.be) beschikt, toegekend door de systeembeheerder.

## *Algemene bepalingen*

Alle personeelsleden worden aangemoedigd e-mail te gebruiken voor het beter uitvoeren van de hen toevertrouwde taken. E-mail is heel geschikt om een vergadering voor te bereiden, en bijvoorbeeld een agenda aan verschillende deelnemers tegelijk te bezorgen.

In principe wordt e-mail enkel gebruikt voor de uitvoering van uw taak.

De personeelsleden zijn individueel verantwoordelijk voor de inhoud van de berichten die zij verspreiden. Binnen nieuwsgroepen kunnen nooit standpunten van het bestuur worden meegedeeld.

Elk personeelslid moet liefst iedere werkdag zijn/haar post opvolgen, behoudens bij afwezigheid t.g.v. het bijwonen van een studiedag en andere dienstprestaties op verplaatsing.

## *Gebruik*

U moet er rekening mee houden dat e-mail zich niet zo goed leent tot het verstrekken van vertrouwelijke informatie. Een kleine manipulatiefout kan ervoor zorgen dat een bericht ongewenst bij de verkeerde personen terechtkomt. E-mailverkeer gebeurt in principe onversleuteld.

## *Langdurig afwezig?*

Bij een geplande afwezigheid van een personeelslid van ten minste twee werkdagen dient het personeelslid de nodige maatregelen te treffen opdat de correspondenten worden verwittigd van zijn/haar afwezigheid, en/of dat de inkomende e-mail automatisch wordt doorgestuurd naar het e-mailadres van een collega van de dienst (in onderling overleg met het diensthoofd).

Bij een niet geplande afwezigheid die langer dan twee werkdagen zal duren, dient binnen de dienst en in overleg met de systeembeheerder een regeling getroffen te worden zodat inkomende e-mail tijdig kan worden behandeld.

## *Uw postbus*

Te veel berichten kunnen het mailsysteem fel belasten en dus vertragen.

U dient dan ook regelmatig onbelangrijke of onbelangrijk geworden berichten uit uw 'postvak in' te verwijderen. Vergeet ook niet de map 'verwijderde items' leeg te maken.

Belangrijke berichten kunnen op een gestructureerde manier worden bijgehouden door in uw 'postvak in' een aantal submappen aan te maken. Zorg ervoor dat deze structuur niet te groot wordt. Belangrijke bijlagen die u wenst te bewaren, kan u beter opslaan op de dataschijf.

Beschikbaarheid van e-mail voor de continuïteit van de dienst

Om in geval van ziekte of vakantie van uzelf of een collega te voorkomen dat de berichten in sommige mailboxen niet behandeld worden, dient u er mee over te waken dat zulke situatie zich niet kan voordoen. Vraag desnoods hulp aan de systeembeheerder om bijvoorbeeld berichten te laten doorzenden aan een collega, om een automatisch antwoord te laten instellen, of om een distributielijst aan te maken. Indien nodig kan een mailbox op dienstniveau worden gemaakt, die door meerdere collega's onafhankelijk van elkaar kan worden opgevolgd.

## *Niet toegestaan*

Volgend gebruik van e-mail is niet toegestaan:

- de loginnaam en het paswoord van iemand anders gebruiken om e-mails te verzenden. Tevens is het niet toegestaan een andere handtekening dan de uwe te gebruiken.
- het wijzigen van het adres van de afzender naar een e-mailadres dat niet toegekend is door het bestuur.
- het is verboden om bij de uitvoering van uw taak gebruik te maken van private adressen (vb. Hotmail of Gmail). Alle elektronische correspondentie die gebruik maakt van de internettoegang, dient te verlopen langs het officiële elektronische adres (dienst@westerlo.be; voornaam.familienaam@westerlo.be).
- een zelfde e-mail naar een grote hoeveelheid ontvangers versturen. Berichten worden gericht verstuurd in functie van de opdracht die moet worden uitgevoerd. De systeembeheerder kan, indien nodig, ingrijpen om verspreiding van kettingmail te beperken of te verhinderen.
- e-mails van grote omvang versturen ( meer dan 8 MB). Voor ontvangers die niet beschikken over een snelle verbinding is dat soms een probleem. Zeer grote bestanden

worden beter eerst gecomprimeerd, zodat ze sneller verstuurd kunnen worden. Soms kan het aangewezen zijn om grote bestanden extern te bewaren, en er een link voor door te sturen. Voor meer informatie kan u bij de systeembeheerder terecht.

- het gebruik van e-mail voor commerciële of illegale doeleinden.
- zich abonneren op elektronische magazines (e-zines) indien dit professioneel niet relevant is.
- inschrijven in mailing lists indien dit professioneel niet relevant is. Dit zorgt voor een te grote belasting van het netwerk.
- Bij het gebruik van e-mail vragen we om geen items te ontvangen waar niet om verzocht is of die niet gewenst zijn. Met items worden in deze context berichten bedoeld met als inhoud creatieve suggesties, kettingbrieven, kunstwerken, grappen, spelvoorstellen, ontwerpen, scripts, behandelingen tegen ziektes, manuscripten, filmpjes, muziek of liedjes, en aanverwante in welke vorm dan ook, van wie dan ook, op welke manier dan ook verstrekt. Zulke berichten verbergen dikwijls een virus of malware. Zodra men zich realiseert dat het ontvangen bericht zulk item is, en als dusdanig een onwelkom idee bevat, moet men dit negeren, het bericht definitief verwijderen (shift+delete) en er geen kopieën van bijhouden.

### *Virusmeldingen*

Het is verboden virusmeldingen naar alle personeelsleden door te sturen. Een door u ontvangen virusmelding stuurt u enkel naar de systeembeheerder en de verantwoordelijke voor informatieveiligheid.

Vaak wordt in virusmeldingen aangeraden om bepaalde, zogenaamd schadelijke bestanden van uw pc te verwijderen. Dit is strikt verboden! Verwijder nooit systeembestanden van uw harde schijf zonder medeweten van de systeembeheerder. Andere berichten vragen u dan weer om net wel op een bepaalde link te klikken. Kijk in zo'n geval altijd eerst naar de link bij een scroll-over. Klik nooit op een link als er iets verdachts aan is. Vraag bij de minste twijfel liever eerst advies van de dienst ict.

### *Controle*

Uw e-mail is in beginsel vertrouwelijk. Dat wil zeggen dat niemand – ook de systeembeheerder of de algemeen directeur niet – kennis neemt van de inhoud van de berichten, tenzij er ernstige/aantoonbare aanwijzingen van misbruik bestaan of indien kennisname nodig is in het licht van de veiligheid van de computerinfrastructuur.

De headers van de berichten (onderwerpregel, afzender of bestemmeling, datum van verzending), evenals de omvang van het elektronisch verkeer kunnen doorgaans wel ingekeken/nagegaan worden.

De systeembeheerder kan omwille van de goede werking van het systeem steeds technische controles (laten) uitvoeren zoals bijvoorbeeld het isoleren of tegenhouden van verdachte berichten, zoals kettingmails en extreem omvangrijke e-mails die een overbelasting of vertraging van het netwerk kunnen teweegbrengen.

### *Representatie*

In uw communicaties waarbij u persoonlijke opvattingen uit, mag u nooit de indruk wekken dat u spreekt namens het bestuur. Hou er rekening mee dat het bericht kan worden doorgestuurd over de hele wereld en dat de naam en faam van ons bestuur verbonden blijft aan zulk bericht wanneer het verzonden wordt via het netwerk van ons bestuur.

### *Doorsturen (forward)*

Wees voorzichtig bij het doorsturen van berichten. Dikwijls worden de e-mailadressen van vroegere bestemmelingen meerdere malen meegestuurd. Op deze manier ontstaat een hele verzendhistoriek, waarvan de e-mailadressen kunnen misbruikt worden voor spam.

### *Bestemmelingen aangeven*

Hoedt u om alle bestemmelingen van een bericht in de hoofding aan: te zetten, omdat daardoor alle bestemmelingen het e-mailadres van alle andere bestemmelingen kunnen zien. Richt het bericht aan uzelf bij aan: en zet alle andere bestemmelingen in bcc:. Zo verspreidt u niet ongevraagd de e-mailadressen van de bestemmelingen.

## 5. Agenda

### *Doelgroep*

Ieder personeelslid die over een toegang tot Outlook beschikt.

### *Algemene bepalingen*

Alle personeelsleden worden aangemoedigd hun agenda te gebruiken voor het beter plannen en uitvoeren van de hen toevertrouwde taken. De elektronische agenda stimuleert het samenwerken in teamverband en het plannen, maar vraagt een gedisciplineerd en consequent bijwerken van de eigen agenda's.

We vragen van alle medewerkers om minstens volgende zaken in hun agenda aan te duiden, en hierbij gebruik te maken van de afgesproken kleurencode:

- alle verlofdagen (rood)
- alle vergaderingen, zowel intern als extern (licht- of donderblauw)

Als je privé-afspraken in je agenda opneemt, kleur ze dan groen.

## 6. Printers, fax en kopieermachines

### *Doelgroep*

Ieder personeelslid in haar of zijn normale werkomgeving.

Algemene bepalingen

Printers en kopieertoestellen zijn uitsluitend beschikbaar voor gebruik in verband met uw taken. Laat geen (zeker geen vertrouwelijke) documenten slingeren bij printers, fax of kopieermachines, maar haal ze steeds dadelijk weg.

Gebruik zonodig de optie om beveiligde (uitgestelde) afdrukken te maken. Je geeft dan een pincode op bij de printopdracht, en je tikt dezelfde code in op de printer om de printopdracht pas te starten, wanneer je ter plaatse bent.

Vooraleer je een document wil printen:

- schat het nodige aantal kopies in
- kies om zoveel mogelijk recto verso te printen
- gebruik kleur enkel wanneer dat nodig is
- vermijd dubbel klassement
- controleer op voorhand (in afdrukvoorbeeld) je tekst op spellingfouten.

Voor privédoeleinden kan printen enkel occasioneel, voor beperkt gebruik en mits afrekening op de kopiedienst aan de tarieven uit het retributiereglement.

## 7. Gebruik van sociale media

U kunt via sociale media deelnemen aan gesprekken over materies waar u als medewerker van de gemeente deskundig in bent. Dat kan een troef zijn voor de organisatie: het kan contacten met de samenleving nauwer en intenser maken en u kunt uw professionele ideeën toetsen aan de realiteit.

Deelname aan sociale media brengt ook een aantal risico's met zich mee, die zowel voor de gemeente als voor u zelf gevolgen kunnen hebben. Belangrijk is dat u ook op sociale media:

- de richtlijnen van de deontologische code in acht neemt,
- verantwoordelijk en loyaal bent
- duidelijk maakt of u in eigen naam spreekt of namens de gemeente.

Deelname aan sociale media is waarschijnlijk niet uw volledige taakinhoud. Vergeet de rest van uw werk niet en gebruik sociale media tijdens de werkuren alleen voor uw werk.

## 8. Mobiel werken en gebruik van VPN

Door telewerken en de moderne informaticamogelijkheden zijn de grenzen tussen privé en werk vaak minder duidelijk. In principe gelden bij mobiel of thuis werken dezelfde veiligheidsmaatregelen als wanneer u vanop uw werkplek zou werken.

Indien u documenten mee naar huis neemt of van thuis uit consulteert, dan treft u de nodige maatregelen om die informatie te beschermen, zowel thuis als onderweg. Het vertrouwelijke karakter van informatie is immers niet plaatsgebonden. U verbindt er zich toe dat de toegang tot het gemeentelijk netwerk van thuis uit enkel door uzelf zal worden gebruikt en erkent dat u de enige geautoriseerde gebruiker bent. U mag uw digitale toegang niet doorgeven of raadpleegbaar te stellen aan gezinsleden of derden en u onderneemt al het nodige om de veiligheid en de privacy van de geconsulteerde documenten te garanderen.

Elk personeelslid heeft de plicht om beveiligingsrisico's en incidenten omtrent de aan hen ter beschikking gestelde middelen, documenten en andere informatie (zoals bijvoorbeeld het verlies van data, opslagmedia of toegang door derden), zonder verwijl te melden aan de dienst ict en de informatieveiligheidsverantwoordelijke.

## 9. Informatieveiligheid

De gemeente beschikt over heel wat informatie en u krijgt die ter beschikking voor de uitvoering van uw taken. Sommige van die informatie is onderworpen aan diverse reglementeringen. Soms stellen we die informatie ter beschikking van de burger in het kader van de openbaarheid van bestuur. Daarnaast is een groot deel van de informatie vertrouwelijk, zoals:

- informatie over zaken waarover de eindbeslissing nog niet gevallen is
- informatie over offertes in het kader van overheidsopdrachten
- persoonsgerelateerde gegevens

U bent verplicht om bij te dragen aan de beveiliging van vertrouwelijke informatie en persoonsgegevens die u verwerkt, aan de integriteit en aan de beschikbaarheid van deze informatie. U behandelt deze informatie op een gepaste wijze en verwerkt ze met gepaste discretie. U waakt erover dat vertrouwelijke informatie niet in verkeerde handen valt. U verandert geregeld uw paswoorden en u verspreidt deze informatie niet ongeoorloofd. U mag geen informatie gebruiken, ook niet anoniem, die u niet nodig heeft voor de uitvoering van uw taken. Deze bepalingen blijven ook gelden wanneer u onze organisatie verlaat.

Bij twijfel neemt u onmiddellijk contact op met uw leidinggevende, de dienst ict en/of de verantwoordelijke voor informatieveiligheid.

# 10. Toezicht en controle

## *Algemene bepalingen*

Het bestuur kan, om eventueel ongeoorloofd gebruik van de communicatiemiddelen door de personeelsleden tegen te gaan, steeds inhoudelijke controles laten uitvoeren, zoals (niet limitatief):

- aantal telefoongesprekken en hun duurtijd
- de adressen van de geraadpleegde websites
- de duur en het ogenblik van de surfsessies
- het aantal en het volume van de uitgaande elektronische mail
- aantal gemaakte copies

## *Algemene uitgangspunten*

- gegevens die tot een persoon herleidbaar zijn, zullen niet worden geregistreerd, verzameld of gecontroleerd, anders dan in deze gedragscode is aangehaald.
- het registreren van gegevens die tot een persoon herleidbaar zijn, wordt tot een minimum beperkt. Hierbij wordt gestreefd naar een maximale bescherming van de privacy van de personeelsleden bij de uitoefening van hun taak en van de gebruikers in het algemeen.
- persoonlijke gegevens zullen alleen gebruikt worden voor het doel waarvoor ze verzameld zijn.

## *Controle door wie en wanneer?*

De systeembeheerder kan omwille van de goede werking van het systeem steeds technische controles (laten) uitvoeren. In de mate dat gegevens moeten worden ingekeken, wordt de vertrouwelijkheid door de systeembeheerder gegarandeerd. Bij vaststelling van zeer ernstige misbruiken en excessen geldt een meldingsplicht aan het toezichthoudend personeel en aan de algemeen directeur.

De diensthoofden en de algemeen directeur kunnen om eventueel ongeoorloofd gebruik van de communicatiemiddelen op te sporen en tegen te gaan, steeds statistische controles – bij wijze van steekproef – laten uitvoeren. Naar aanleiding van dergelijke statistische verificatie zullen de gebruikers geïnformeerd worden, indien bepaalde sites, waarvan de inhoud niet verenigbaar is met deze gedragscode, werden bezocht.

Na een vaststelling van onrechtmatig gebruik, kunnen deze inhoudelijke controles op herhaalde tijdstippen worden uitgevoerd.

Indien er gegronde aanwijzingen zijn die doen vermoeden dat er misbruik wordt gemaakt van de werkinstrumenten, kan de identiteit van de gebruiker worden nagegaan. Dit is enkel toegestaan indien er geen andere mogelijkheden zijn om dit misbruik aan te tonen. Het bestuur zal hierbij steeds de algemene uitgangspunten respecteren.

## *Mogelijkheid tot rechtvaardiging van de handelingen*

Het personeelslid van wie gevraagd wordt het internetverkeer te onderzoeken, wordt hiervan op de hoogte gesteld door het diensthoofd of de personeelsdienst.

Voor toegang tot een site, waarvan de inhoud niet verenigbaar is met deze gedragscode, om professionele redenen, neemt u best op voorhand contact op met uw diensthoofd of met de algemeen directeur.

# 11. Sancties

## *Algemene bepalingen*

In de gevallen waarbij door het oneigenlijk gebruik van netwerk- en computersystemen schade en/of verlies van gegevens dreigt, behouden de systeemverantwoordelijken zich het recht voor om in te grijpen in die netwerk- en computersystemen, teneinde verder onheil te voorkomen. Het afsluiten van de netwerk- en internettoegang kan hierbij als bewarende maatregel ingesteld worden.

Onverminderd de eventuele toepassing van de statutair voorziene tuchtregeling, kunnen overtredingen van ernstige aard leiden tot het opschorten of beperken, gedurende kortere of langere periode, van de gebruiksrechten van de netwerkdiensten. Het personeelslid waarop dit wordt toegepast, wordt hiervan vooraf in kennis gesteld.

Deze maatregelen kunnen worden toegepast voor alle gebruikers.

## *Mogelijke sancties*

Indien ongeoorloofd gebruik van de communicatiemiddelen wordt vastgesteld, dan kan het bestuur alle maatregelen nemen die voorzien zijn in het personeelsstatuut.

Afhankelijk van de overtreding kan een ordemaatregel genomen worden of een tuchtstraf opgelegd worden.