# GEMEENTE EN OCMW DEERLIJK

# REGLEMENT MOBIELE WERKINSTRUMENTEN

## A. Inleiding

Gemeente en OCMW Deerlijk zetten in op flex- en telewerk en voorzien daarom in de nodige middelen om elke medewerker maximaal te faciliteren in hun job en hen in de mate van het mogelijke de kans te geven om plaats- en tijdsonafhankelijk te werken. Dit impliceert dat de apparatuur die ter beschikking wordt gesteld ook een mobiel karakter vraagt om zowel binnen de locaties van de organisatie (eigen bureau, flexwerkplekken of op andere diensten), op verplaatsing of thuis te kunnen werken.

Het bestuur moedigt expliciet het gebruik van de voorziene middelen aan met de bedoeling om de werkproductiviteit en -kwaliteit te maximaliseren. Tegelijk investeren we in de noodzakelijke technische beschermingsmiddelen om zowel de gebruiker als het netwerk van de organisatie te behoeden voor internetmisbruiken, virussen, malware, phishing, ransomware, hacking, e.d. In deze heeft ook elke medewerker een belangrijke verantwoordelijkheid.

Het opzet van dit reglement, dat deel uitmaakt van het arbeidsreglement, is om duidelijke afspraken te maken rond het gebruik van de middelen. We streven een evenwicht na tussen enerzijds de bescherming van de persoonlijke levenssfeer van de gebruikers, en anderzijds de wettelijke controle uitgeoefend door het bestuur op het gebruik van de ICT-infrastructuur.

## B. Werkstations (desk- en laptops)

### 1. Algemeen

*Artikel 1*

Het bestuur voorziet elke medewerker van wie de functie het vereist een kwalitatief, performant en beveiligd werkstation, wat in regel in de vorm van een laptop is. Het werkstation, ongeacht of dit in de vorm van een desk- of laptop is, blijft te allen tijde de eigendom van het bestuur. De gebruiker krijgt dit toestel om de hem/haar toevertrouwde functie te kunnen uitoefenen en wordt geacht hier met de nodige zorg en respect mee om te gaan. Het feit dat het werkstation een mobiel karakter heeft, doet niets af van de omgangspraktijken die ook gelden voor niet-mobiele werkapparatuur.

*Artikel 2*

Elk werkstation is gekoppeld aan de functiehouder, en wordt voorzien van persoonlijke logingegevens die de functionaliteiten van het toestel, de rechten op bedrijfssoftware en toegang tot het netwerk

bepalen zoals ingesteld door de IT-dienst. Het is dan ook in geen geval toegestaan om aan een derde persoon toegang te geven tot het toestel, het netwerk van het bestuur en de bijhorende toepassingen op welke wijze dan ook, tenzij een wet of regelgeving hiertoe verplicht. Intern kan het toestel tijdelijk gebruikt worden door een collega in uitzonderlijke noodsituaties, of bij een interventie van de IT-dienst. Elke medewerker heeft aldus een persoonlijke verantwoordelijkheid om geen oneigenlijk gebruik van het toestel toe te laten.

*Artikel 3*

De laptops die door het bestuur ter beschikking worden gesteld, worden in hun volledigheid beheerd door de IT-dienst zoals vermeld in artikel 2. Het is door de gebruiker niet toegelaten om eigen software, toepassingen of configuraties aan het toestel te doen, en dit wordt in se ook onmogelijk gemaakt door de administratorrechten van het toestel op niveau van de IT-dienst te plaatsen. Dit dient ter waarborging van het strikt professioneel gebruik van het toestel.

*Artikel 4*

Het gebruik van de "restmogelijkheden" van het toestel, het gebruik van internet en e-mail worden als volgt vastgelegd:

*Toegelaten gebruik:*

Het aanbod aan informatie en diensten op het internet is groot en aantrekkelijk. Nochtans is, in een werkkader, in principe slechts een professioneel gebruik, uitsluitend ten behoeve van het bestuur, toegelaten.

Inzake e-mail, moet elk extern bericht steeds voorzien zijn van een visuele handtekening. De handtekening dient minimaal een aantal vermeldingen te bevatten conform de huisstijl, zoals naam, voornaam, functie, coördinaten. De handtekening wordt automatisch gegenereerd vanuit de backoffice door de IT- en communicatiedienst. Eigen ontworpen handtekeningen worden niet gedoogd.

Internetexploratie voor de persoonlijke ontwikkeling is tijdens de pauzes evenwel toegestaan, maar mag in geen geval de goede werking van het netwerk of de productiviteit van het personeelslid verstoren.

E-mail kan tijdens de pauzes zonder voorafgaande toestemming gebruikt worden voor privédoeleinden.

Het gebruik van internet en e-mail kan enkel onder volgende voorwaarden:

- het gebruik is occasioneel;
- het gebruik belemmert op geen enkele manier de goede werking van de dienst en de productiviteit;

- het gebruik houdt geen schending in van deze richtlijnen, de wettelijke bepalingen, de arbeidsovereenkomst en/of het arbeidsreglement.

*Verboden gebruik:*

De personeelsleden dienen zich te onthouden van elk gebruik van het internet- en e-mail dat niet overeenstemt met het gebruik ervan door een normaal, zorgvuldig gebruiker of dat indruist tegen de principes van deze richtlijnen of dat in strijd is met de instructies die door het bestuur worden gegeven. Vanuit de IT-dienst wordt de toegang voor zover mogelijk en beheersbaar tot bepaalde websites die een risico kunnen vormen voor het eigen netwerk alsook de persoonlijke integriteit van de medewerker, geblokkeerd. Het ontbreken van een blokkering, betekent in geen geval de goedkeuring van het gebruik van dergelijke websites.

Zonder limitatief te zijn, worden volgende activiteiten in ieder geval ten strengste verboden, zelfs in het kader van de uitvoering van de functie:

- vertrouwelijke informatie over het bestuur, zijn opdrachten of zijn personeel verspreiden, behalve indien de functie dit op een redelijke manier eist;
- gegevens verspreiden of downloaden die beschermd zijn door auteursrechten en die bij de wet beschermd zijn tegen schending;
- berichten doorsturen of sites bezoeken waarvan de inhoud de waardigheid van de anderen in gevaar kan brengen, namelijk het doorsturen of bezoeken van racistische of revisionistische sites, of sites die discriminerend zijn op basis van geslacht, seksuele geaardheid, handicap, godsdienst of politieke overtuigingen van een persoon of een groep personen; verzenden van berichten die beschouwd worden als pornografisch, of bezoeken van erotische of pornografische sites, zelfs als ze bij de wet toegestaan zijn;
- berichten, beelden of bijlagen doorsturen of op aanvraag ontvangen, die door het volume de goede werking van de IT-infrastructuur kunnen beïnvloeden;
- persoonlijke interne of externe berichten doorsturen die niets te maken hebben met de functie gezien de belangrijke risico's die deze kunnen inhouden (lijnen blokkeren, virussen verspreiden, …);
- "uitvoerbare" bestanden (exe-, com-bestanden, …), doorsturen en/of, in geval van ontvangst, openen; deze vormen immers een ernstige bedreiging voor de stabiliteit en de veiligheid van het netwerk;
- aan "kettingbrieven" meewerken;
- meer algemeen, zowel de interne als de externe elektronische briefwisseling of het internet gebruiken voor een illegale activiteit, van om het even welke aard;
- het verzenden van provocerende e-mails;
- het gebruik van e-mails om bepaalde situaties binnen het bestuur openlijk aan te klagen;
- het verzenden van e-mails waarin wordt aangezet tot het plegen van strafbare feiten;
- het verzenden van berichten die verband houden met spelen en weddenschappen, verdovende middelen of vormen van fraude;

- elk gebruik van het e-mailsysteem in het kader van een onwettige activiteit, welke ook, of in strijd met wettelijke bepalingen. De gebruikers worden dienaangaande gewezen op de verplichtingen die voortvloeien uit de Wet van 28 november 2000 inzake computercriminaliteit, dat o.m. volgende feiten strafbaar stelt (art. 550bis Strafwetboek):
    - kennisname van informaticagegevens van personeelsleden door gebruik van andermans wachtwoord;
    - kennisnemen van informaticagegevens van personeelsleden of derden door het zich toegang te verschaffen tot een netwerk, een server of een bestand zonder daartoe de toestemming te hebben ("hacking");
    - kennisname van door hacking verkregen gegevens.

  Bij twijfel aangaande de geoorloofdheid van een gebruik van e-mail, dient het personeelslid zich te wenden tot zijn/haar rechtstreekse leidinggevende.
  Het bestuur behoudt zich het recht voor om op elk ogenblik de toegang tot bepaalde of alle sites te verbieden, waarvan de inhoud onwettig, beledigend of onaangepast zou zijn, of meer algemeen vreemd zou zijn aan de activiteiten van het bestuur.

## 2. Veiligheidsmaatregelen

*Artikel 5*

Elk werkstation is een poort tot het netwerk van de organisatie, wat een strikt professioneel gebruik van het toestel vereist. Enkel de dienst IT of aangestelde derden hebben toestemming voor het installeren, demonteren, verplaatsen of wijzigen van het informaticamateriaal. Enkel hardware/software die door de IT-dienst ter beschikking werd gesteld, mag gebruikt worden.

*Artikel 6*

Aansluitingen op externe netwerken zoals het internet, die niet toegelaten zijn door de aanstellende overheid, of die geïnstalleerd noch geconfigureerd zijn door de dienst IT, zijn strikt verboden.

Het gebruik van aansluitingen op externe netwerken en van e-mail moet beperkt blijven tot verrichtingen die absoluut noodzakelijk zijn voor de goede werking van de diensten.

*Artikel 7*

De gebruikers van het informaticamateriaal aangesloten op het netwerk worden verzocht hun bestanden op te slaan op de door het bestuur daarvoor voorziene opslagmogelijkheden (i.e. de eigen server en of de cloudmogelijkheden binnen de eigen O365-omgeving). De toegang tot deze gegevens en de verdeling ervan onder verschillende gebruikers wordt geconfigureerd door de dienst IT volgens de behoeften van de betrokken diensten.

*Artikel 8*

Indien het informaticamateriaal abnormaal functioneert, moet de dienst IT onmiddellijk verwittigd worden en mag dit materiaal niet meer gebruikt worden. Enkel de dienst IT en de informatici van de leveranciers zijn bevoegd tussen te komen voor het materiaal, de geïnstalleerde programma's en hun

configuraties. De IT-dienst kan de gebruiker steeds toestemming geven om bepaalde handelingen uit te voeren die en oplossing kunnen bieden.

De gebruiker waakt ook over het onderhoud van het toestel door de voorgestelde updates uit te voeren en het toestel correct af te sluiten.

**Controlemodaliteiten**

*Artikel 9*

Het bestuur behoudt zich het recht voor om op elk ogenblik algemene controles uit te voeren over het gebruik, per personeelslid, van het internet en/of van e-mail.

De controle zal worden uitgeoefend voor gerechtvaardigde doeleinden, en met name met het oog op het nastreven van één of meerdere van de volgende doeleinden:

1. het voorkomen van ongeoorloofde of lasterlijke feiten, feiten die strijdig zijn met de goede zeden of de waardigheid van een andere persoon kunnen schaden;
2. de bescherming van de belangen van het bestuur die een vertrouwelijk karakter hebben en het tegengaan van praktijken die ermee in strijd zijn;
3. de veiligheid en/of de goede technische werking van de IT-netwerksystemen van het bestuur, met inbegrip van de controle op de kosten die ermee gepaard gaan alsook de fysieke bescherming van de installaties van het bestuur;
4. het te goeder trouw naleven van de in het bestuur geldende beginselen en regels voor het gebruik van online technologieën, zoals vermeld in het arbeidsreglement, onderhavig reglement, de arbeidsovereenkomst of enige andere reglementaire of contractuele bepaling.

Het bestuur zal bij de controle de eerbied voor het privéleven van het personeelslid in acht nemen en zal bij de controle niet verder gaan dan wat proportioneel evenredig is voor het verwezenlijken van deze doelstellingen.

*Artikel 10*

*Waarom worden de gegevens verzameld?*

De bedoeling van de gegevensverzameling in dit reglement is om een controle te kunnen uitoefenen op het internet- en e-mailgebruik overeenkomstig de hier vermelde bepalingen, zodanig dat de taken die aan een personeelslid of aan een dienst toevertrouwd worden, op een goede manier volbracht kunnen worden.

Deze verzameling heeft eveneens tot doel te controleren of het gebruik geen schending betekent van om het even welke wettelijke bepaling, de arbeidsovereenkomst, de rechtspositieregeling of het arbeidsreglement dat van kracht is op het personeelslid.

*Hoe worden de gegevens verzameld?*

In het kader van deze controle worden enkel elektronische communicatiegegevens verzameld die toereikend zijn, terzake dienend en niet overmatig zijn met betrekking tot het doel dat wordt nagestreefd of een ander doel dat hiermee verenigbaar is.

Het betreft algemene informatie, zoals gegevens over:

- de adressen van geraadpleegde websites;
- de duur en het ogenblik van verbinding;
- het aantal en het volume van de uitgaande elektronische mail per werkpost;
- …

Indien dit algemeen toezicht geen enkel misbruik of geen enkele onregelmatigheid aantoont, zullen de gegevens onmiddellijk vernietigd worden. Indien de controle wel misbruik of onregelmatigheden aantoont, worden de gegevens gedurende een periode van zes maanden bewaard door de algemeen directeur.

In geen geval kan het overnemen van individuele schermen van personeelsleden door de dienst IT als algemeen toezicht beschouwd worden. Om hiertoe over te gaan zal de dienst IT steeds toestemming dienen te vragen aan het personeelslid. Doen ze dit niet, dan stelt men zich bloot aan de sancties zoals opgesomd in artikel 11 van deze bijlage.

*Hoe worden de gegevens geïndividualiseerd?*

Wanneer het bestuur tijdens een controle een onregelmatigheid vaststelt, zullen de verzamelde communicatiegegevens worden verwerkt om ze aan een geïdentificeerde of identificeerbare persoon toe te schrijven.

Communicatiegegevens waarvan het beroepsmatig karakter door het personeelslid niet in twijfel wordt getrokken, kunnen steeds het voorwerp uitmaken van een individualisering.

De individualisering van privé communicatiegegevens kan direct of indirect zijn naargelang het doel van de controle.

Ter zake geldt volgende procedure:

- Voorlichtingsfase: voorafgaand aan de individualisering zal het personeelslid worden ingelicht op een duidelijke en begrijpelijke wijze over het bestaan van de onregelmatigheid en over het feit dat de elektronische online communicatiegegevens geïndividualiseerd zullen worden indien een nieuwe onregelmatigheid wordt vastgesteld;
- Individueel onderhoud: wanneer opnieuw een onregelmatigheid wordt vastgesteld en wanneer het personeelslid bij toepassing van de procedure inzake individualisering verantwoordelijk wordt bevonden voor een onregelmatigheid bij het gebruik van de elektronische online communicatiegegevens, wordt het geïdentificeerd personeelslid door het bestuur uitgenodigd

voor een gesprek. Tijdens dit gesprek vermeldt het personeelslid, eventueel bijgestaan door een vakbondsafgevaardigde, zijn bezwaren tegen de vooropgestelde maatregel (sanctie) en geeft hij uitleg over zijn gebruik van de informaticamiddelen die hij ter beschikking heeft.

Het personeelslid heeft het recht kennis te nemen, na afspraak, van elk gegeven hem betreffende dat zou worden verzameld bij een dergelijke controle.

Indien een gegeven niet correct blijkt te zijn, verbindt het bestuur zich ertoe de nodige verbeteringen aan te brengen.

**Sancties**

*Artikel 11*

Naar aanleiding van elke inbreuk van een personeelslid op deze richtlijnen kan het bestuur - na verloop van voormelde procedure – de nodige maatregelen treffen.

Voor de statutaire personeelsleden is dit de tuchtprocedure. Voor de contractuele personeelsleden is de wet op de arbeidsovereenkomsten van toepassing.

Concreet betekent dit:

- schriftelijke verwittiging
- ontslag met opzegtermijn
- ontslag om dringende reden.

**Opvolging**

*Artikel 12*

De naleving van deze richtlijnen zal opgevolgd worden door de IT-verantwoordelijken. Bij deze personen kunnen alle personeelsleden terecht voor eventuele vragen, opmerkingen, klachten of suggesties. Het bestuur garandeert een strikt vertrouwelijke behandeling van klachten. Overleg met de betrokkene staat hierbij centraal.

Op basis van input van medewerkers kunnen voorstellen gedaan worden voor eventuele aanpassingen / vervolledigingen van deze richtlijnen.

**Goede aanbevolen praktijken**

*Artikel 13*

Het internet is in de eerste plaats een instrument voor dialoog en openheid. Zijn academische en informele bronnen hebben er een "gebruiksetiquette" van gemaakt: een "Netiquette".

De diensten moeten zich organiseren zodat hun mailbox dagelijks wordt gecontroleerd en een ontvangstbewijs dient zo vlug mogelijk te worden toegestuurd als de vraag niet onmiddellijk (binnen 2 werkdagen) kan worden beantwoord.

Naast de hierboven vermelde voorschriften, moeten de volgende punten in acht genomen worden:

- geen enkel bericht onbeantwoord laten;
- zich niet laten meeslepen in polemieken;
- steeds hoffelijk blijven, zelfs tegenover brutale berichten;
- geen opmerkingen maken over personen, enkel over onderwerpen;
- e-mails opstellen volgens de huisstijl van het bestuur en in courante lettertypes;
- geen elektronische berichten naar anderen doorsturen ("forward") wanneer er geen gerechtvaardigde professionele reden bestaat, bijvoorbeeld bij omstandigheden waarin afbreuk gedaan wordt aan de persoon die het originele bericht geschreven heeft.

De door te geven informatie moet duidelijk en gecontroleerd zijn: deze informatie mag geen aanleiding geven tot verwarring of vergissingen. De informatie die op het internet te vinden is, is niet altijd correct; ze moet eerst gecontroleerd worden en daarna pas bevestigd of verspreid. De informatieverspreiding op het internet is niet vertrouwelijk. De gevolgen in verband met de intellectuele eigendom van deze verspreiding zijn dezelfde als die van een publicatie van elke andere vorm.

## C. Smartphones en GSM's

***Toestellen***

*Artikel 14*

Het bestuur stelt een smartphone of GSM met abonnement ter beschikking van personeelsleden voor wie dit noodzakelijk wordt geacht in de uitoefening van de functie. Het type toestel en het abonnement wordt bepaald door de IT-dienst, rekening houdende met de noodzakelijke functionaliteiten en veiligheidsvereisten, en blijft eigendom van het bestuur. Bij het beëindigen van de tewerkstelling bij het bestuur, wordt het toestel teruggegeven.

De medewerker draagt de nodige zorgen voor het toestel. Eventuele schade of haperingen worden onmiddellijk gemeld. Een medewerker kan aansprakelijk gesteld worden voor schade aan de apparatuur door nalatigheid of onachtzaamheid.

Een personeelslid kan door middel van de dual sim mogelijkheid een persoonlijke sim-kaart inbrengen via dewelke privé-gebruik kan gebeuren. Bij gebruik van dual sim, waarbij het privatief gebruik kan aangetoond te worden door middel van eigen facturen, is er geen voordeel alle aard (cfr. Artikel 18).

*Artikel 15*

Het bestuur kan ook een toestel ter beschikking stellen van een dienst of ploeg. Dergelijke toestellen zijn niet gekoppeld aan een individu, en dienen de bereikbaarheid van de dienst te maximaliseren

wanneer deze onderweg zijn. Een dergelijk toestel dient uitsluitend voor professioneel gebruik en kan niet privé gehanteerd worden.

*Artikel 16*

Het personeelslid kan opteren om een eigen toestel gebruiken, al dan niet met een abonnement door het bestuur voorzien, en dient in dat geval de aankoopkost zelf te dragen. Ook bijkomende accessoires (hoesjes, handsfree kit, oortjes, screen protectors, …) zijn voor eigen rekening. Voor een dergelijk toestel wordt geen voordeel alle aard aangerekend

De medewerker draagt de volledige verantwoordelijkheid voor het eigen toestel. Bij verlies, diefstal of defect is er geen tussenkomst van het bestuur.

**Limieten**

*Artikel 17*

Het bestuur neemt abonnementen af via het raamcontract van de Vlaamse Overheid. Met deze abonnementen kan gratis gebeld worden naar (nationale) vaste nummers, en GSM-nummers die tot de organisatie behoren. Het overig gebruik, zijnde internationaal bellen en bellen naar andere mobiele nummers, gebeurt tegen betaling.

Er worden twee belprofielen gehanteerd:

- Profiel A (= standaardprofiel)
    - Dit profiel voorziet 2GB aan data wat als de minimale voorwaarde wordt beschouwd om, bij afwezigheid van een WiFi-verbinding, gebruik te kunnnen maken van O365 en andere webtoepassingen.
    - Dit profiel voorziet tevens 10 euro belwaarde.
- Profiel B (= uitgebreid profiel)
    - Dit profiel voorziet 5GB aan data. Deze mogelijkheid wordt voorzien voor leden van het MAT en de IT-dienst gezien deze doorgaans een hoger datagebruik kennen wegens het regelmatig werken vanop diverse locaties.
    - Dit profiel voorziet tevens 15 euro belwaarde.

Inzake het datagebruik dient elk personeelslid erover waken om maximaal gebruik te maken van WiFi indien die aanwezig is. Enkel in de gevallen waar geen WiFi voor handen is, wordt de data geacht gebruikt te worden.

In individuele gevallen kan geopteerd worden om ofwel de data, ofwel de belwaarde, ofwel beide te verhogen, in functie van de professionele context, voor zover een duidelijke motivatie wordt aangeleverd.

Voordeel alle aard

*Artikel 18*

Het toestel en/of het abonnement dat wordt voorzien dient in regel voor professioneel gebruik.

Voor bepaalde profielen kan ook een privaat gebruik toegestaan worden, in welk geval er een voordeel alle aard ontstaat in hoofde van het personeelslid, waarop sociale zekerheidsbijdrage en bedrijfsvoorheffing zijn verschuldigd. Een dergelijk privatief gebruik is in regel mogelijk voor leden van het managementteam, en de IT-dienst.

*Artikel 19*

Indien de medewerker niet over een eigen toestel met privé-abonnement beschikt, wordt er van uit gegaan dat er zowel een privé- als beroepsgebruik is. Hierdoor gaat de medewerker akkoord met het voordeel alle aard die maandelijks van het maandloon in mindering zal gebracht worden.

Indien de medewerker wel over een eigen toestel met privé-abonnement beschikt, en dit als zodanig verklaart, dan dient er geen voordeel alle aard aangerekend te worden. In dit geval wordt er van uit gegaan dat er enkel een beroepsmatig gebruik is. Bijkomende voorwaarde is dat de medewerker zelf de privéfacturen bijhoudt gedurende 3 jaar en deze ook kan voorleggen bij een eventuele RSZ-controle. Indien de medewerker deze niet kan voorleggen, dan zullen eventuele regularisaties voor zijn/haar eigen rekening zijn.

*Artikel 20*

Buitenlandse gesprekken kunnen door het bestuur teruggevorderd worden aan de medewerker, indien deze niet kan aantonen dat deze noodzakelijk waren voor de uitvoering van zijn/haar functie.

Wanneer de financiële dienst of de leidinggevende buitensporige kosten vaststelt, zal een verklaring gevraagd worden. Bij gebrek aan een geldige reden zullen deze tevens teruggevorderd worden van de medewerker.

*Artikel 21*

Ingeval van diefstal van de smartphone doet de medewerker hiervan aangifte bij de politie en verwittigt hij/zij de IT-dienst om het toestel te blokkeren. De medewerker bezorgt een kopie van het proces-verbaal aan de IT-dienst.

*Artikel 22*

Bij het beëindigen van de arbeidsovereenkomst of de aanstelling, het opnemen van volledige langdurige verlofstelsels of bij andere langdurige afwezigheden van > 6 maand zal de medewerker zijn/haar toestel, samen met alle toebehoren, inleveren bij de IT-dienst. In specifieke gevallen kunnen hierop uitzonderingen worden toegestaan.

*Artikel 23*

Bij ingebruikname van een GSM, smartphone, telefonie- en/of data-abonnement ondertekent de medewerker een verklaring op eer waarbij hij/zij diens keuze aangeeft ten opzichte van het voordeel alle aard.

**Informatieveiligheid**

*Artikel 24*

Elke medewerker die een smartphone gebruikt, zorgt ervoor dat de toegang steeds beveiligd wordt met een wachtwoord, vingerafdruk en/of gezichtsherkenning zodat in geval van verlies of diefstal geen werkdata kunnen worden gerecupereerd door derden.