C·SMART

# ICT-policy

**Lokaal Bestuur Wommelgem**
**versie 10/2024**

LOKAAL DIGITAAL

# Inhoud

## Draagwijdte en toepassingsgebied

**Art.1** Deze ICT-policy is een intern reglement en heeft een afdwingbaar karakter.

**Art.2** Deze ICT-policy is ondergeschikt aan dwingende wetsbepalingen en hun uitvoeringsbesluiten.

**Art.3** Deze policy regelt de toegang, het intern en extern gebruik en de controle van de ICT-infrastructuur die door het bestuur ter beschikking wordt gesteld van de gebruiker. Bedoeld worden onder andere de computer- en netwerkinfrastructuur (hardware en software), cloud-omgevingen, e-mail, internet, intranet, printers, kopieermachines, telefonie, gsm, smartphone evenals eventueel toekomstige elektronische media.
Deze policy geldt eveneens voor alle gegevens die via deze systemen worden geproduceerd, overgedragen of erin worden opgeslagen.

**Art.4** Deze ICT-policy is van toepassing op alle gebruikers van de ICT-infrastructuur. Onder gebruiker wordt verstaan de personeelsleden, vrijwilligers, stagiairs, mandatarissen en iedereen die in contact komt met de ICT-infrastructuur.

## Eigendom en verantwoordelijkheid

**Art.5** De ICT-infrastructuur die de gebruiker ter beschikking is gesteld, blijft eigendom van het bestuur. De gebruiker ondertekend een gebruikersovereenkomst per toestel dat hij ontvangt. Bij langdurige afwezigheid kan het ter beschikking gestelde ICT materiaal en andere hulpmiddelen (vb. smartphone, laptop…) teruggevraagd worden en toegangen geblokkeerd worden.

**Art.6** De gebruiker draagt als een goede huisvader zorg voor de ICT-infrastructuur die hem ter beschikking is gesteld. Hij gebruikt deze middelen op een professioneel, sociaal, ethisch en juridisch correcte wijze, overeenkomstig de bepalingen in deze policy en de instructies die ter zake worden gegeven.

**Art.7** De gebruiker mag geen software die ter beschikking gesteld wordt door het bestuur transfereren naar eigen apparatuur, behoudens toestemming van het bestuur of diens afgevaardigde.

**Art.8** Elke gebruiker is verantwoordelijk voor zijn communicatiegedrag.

**Art.9** Het bestuur is niet verantwoordelijk voor misdrijven die door personeelsleden worden begaan.

## Toegang en bescherming

**Art.10** <u>Gebruikersnaam en wachtwoord</u>

§1 De toegang tot de ICT-infrastructuur wordt verleend op basis van een gebruikersnaam en een wachtwoord en waar mogelijk een tweestapsverificatie.

§2 De gebruiker mag uitsluitend met zijn eigen gebruikersnaam en wachtwoord inloggen. Het is niet toegestaan de gebruikersnaam en het wachtwoord van iemand anders te gebruiken, behalve indien de continuïteit van de dienstverlening in het gedrang komt en niet op een andere manier kan worden gegarandeerd.

§3 Elke gebruiker is verantwoordelijk voor het bewaren van zijn gebruikersnaam en wachtwoord. Dit betekent dat hij erop let dat zijn wachtwoord geheim blijft. Om dit te

garanderen, gebruikt hij een wachtwoord dat moeilijk te kraken is en wordt hij verplicht dit periodiek te veranderen.

§4 Niemand mag zijn gebruikersnaam of wachtwoord aan onbevoegden doorgeven en/of door onbevoegden laten gebruiken.

§5 Gebruikers met toegang tot externe databanken (zoals Kruispuntbank sociale zekerheid, rijksregister, enz.) verbinden zich ertoe de veiligheidsvoorschriften en richtlijnen in het kader van de aansluiting tot deze strikt na te leven.

In het kader van onze IT-beveiliging is het verplicht voor medewerkers om Multi-Factor Authenticatie (MFA) in te stellen voor hun werkaccount. Medewerkers die geen werktelefoon van het lokaal bestuur hebben, dienen hiervoor hun privé mobiele telefoon te gebruiken. Dit biedt een extra beveiligingslaag en zorgt voor snelle waarschuwingen bij onregelmatige inlogpogingen, wat essentieel is voor de bescherming van bedrijfsinformatie. Medewerkers zonder geschikte privé telefoon kunnen contact opnemen met de IT-afdeling voor alternatieve oplossingen.

**Art.11** De gebruiker neemt de nodige veiligheidsmaatregelen om schade aan de ICT-infrastructuur te voorkomen, zowel binnen het bestuur als daarbuiten. Draagbare ICT-infrastructuur (laptop, gsm,...) mag nooit onbewaakt op een openbare plaats of zichtbaar in een voertuig worden achtergelaten.

**Art.12** De gebruiker vergrendelt steeds zijn PC, laptop of tablet als hij zijn werkruimte verlaat door gelijktijdig op de Windows-toets en L te duwen. Automatisch gaat het toestel over op schermbeveiliging na 15 minuten.

**Art.13** De gebruiker print uitgesteld. Hij laat geen afgedrukte documenten achter bij de printer.

**Art.14** De gebruiker sluit dagelijks na gebruik zijn PC af, ook bij transport wordt de laptop afgesloten.

**Art.15** De gebruikers waken erover om zuinig om te springen met schijfruimte op de server en de lokale computer zorgen ervoor dat overbodige bestanden regelmatig verwijderd worden. Elke gebruiker is verantwoordelijk voor (of volgt de richtlijnen m.b.t.) de informatie die hij beheert en voor de informatie die hij opvraagt.

**Art.16** <u>Beveiliging</u>

§1 De gebruiker moet de geïnstalleerde beveiligingssoftware gebruiken en alle richtlijnen in dit verband opvolgen. De gebruiker mag de beveiligingssoftware niet wijzigen of uitschakelen.

§2 Bij het gebruik van eigen opslagmedia (diskettes, cd-roms, dvd's, memorysticks (USB),…) op de ICT-infrastructuur van het bestuur, moeten deze vooraf gescand worden op virussen.

§3 De gebruiker mag nooit zelf proberen virussen te vernietigen en moet de ICT verantwoordelijke verwittigen.

**Art.17** <u>Incident melden</u>

De data protection officer (DPO) moet zo snel mogelijk op de hoogte worden gebracht bij elk incident in verband met de veiligheid of elke ontdekte tekortkoming in de beveiliging van de ICT-infrastructuur waardoor de vertrouwelijkheid, de integriteit en/of de beschikbaarheid van de informatie of het informatiesysteem in het gedrang kunnen komen. In dat geval is de gebruiker tot geheimhouding tegenover anderen gebonden. Via privacy@c-smart.be meld u dit rechtstreeks aan onze externe DPO, meldingen mogen ook steeds gemeld worden via ict@wommelgem.be.

**Art.18** Het bestuur of zijn afgevaardigde kan de toegang tot (bepaalde) websites verhinderen.

**Art.19** Met het oog op de continuïteit van de dienstverlening kan de algemeen directeur in geval van overmacht of in uitzonderlijke omstandigheden informatie, systemen, bestanden of gegevens die essentieel zijn en die niet langer op een andere wijze beschikbaar zijn, laten lokaliseren en recupereren.

## Beroepsmatig en persoonlijk gebruik

### Beroepsmatig gebruik

**Art.20** De gebruiker kan binnen de grenzen van deze policy vrij gebruik maken van de ICT-infrastructuur die hem ter beschikking is gesteld in functie van de uitvoering van de opdrachten die hem door het bestuur zijn toevertrouwd.

### Persoonlijk gebruik

**Art.21** De gebruiker heeft de keuze om ofwel privé gebruik te maken van het toestel en hiervoor voordeel alle aard te betalen ofwel uitsluitend gebruik te maken van het toestel voor zakelijke doeleinden.

De ICT-infrastructuur kan voor privédoeleinden gebruikt worden voor zover:

- voordeel alle aard betaald wordt
- dit gebeurt buiten de werkuren van de gebruiker;
- ervoor gezorgd wordt dat er een strikte scheiding is tussen privé en werk data zoals bijv. een privé map voorzien in de folder documenten;
- dit geen gevolg heeft voor de goede werking van de infrastructuur.

**Art.22** De gebruiker doet alle mogelijke inspanningen om te vermijden dat er privémails door derden aan hem worden gericht op een officieel mailadres van het bestuur.

### Digitale communicatie

**Art.23** E-mail

§1 Alle e-mailverkeer verloopt via de officiële adressen van het bestuur. E-mail kan enkel gebruikt worden als communicatiemiddel, bevestiging van een telefoongesprek, enz. en heeft op zich geen bindend karakter. Officiële verbintenissen worden gedagtekend en ondertekend door de burgemeester en de algemeen directeur. Het gebruik van de officiële adressen van het lokaal bestuur voor privé-doeleinden is verboden. Het e-mailsysteem is niet bedoeld voor het archiveren van belangrijke informatie. Als gebruikers e-mailgegevens wensen te bewaren, dan moeten ze die archiveren door op te slaan en aan het elektronisch dossier toevoegen. Gebruikers mogen enkel het aan hen toegewezen e-mail account gebruiken.

§2 Afwezigheid

De gebruiker moet tijdens zijn afwezigheid een automatisch antwoord instellen met de nodige contactgegevens en de gepaste maatregelen nemen ten einde de continuïteit te verzekeren.

§3 Geplande afwezigheid

Bij geplande afwezigheid stelt de gebruiker zelf een automatisch antwoord in waarmee een afzender in kennis gesteld wordt van diens afwezigheid met vermelding van de geschikte persoon aan wie de boodschap gericht kan worden, indien deze niet kan wachten tot de terugkeer van de afwezige medewerker.

§4 Niet-geplande afwezigheid

De leidinggevende wordt gemachtigd om de berichten en professionele bestanden te

raadplegen, ingeval van gerechtvaardigde noodzaak en hoogdringendheid, die niet toelaat om de terugkeer van de medewerker af te wachten.

§5 Authenticiteit van de inkomende berichten (phising)
De gebruikers van informatietechnologieën erkennen dat bepaalde informatie enkel voor specifieke personen bestemd is en niet algemeen mag worden verspreid. De gebruikers houden er rekening mee dat adressen van verzenders en bestemmelingen van de externe berichten vervalst kunnen zijn en dat bijgevolg de authenticiteit van deze berichten niet altijd gewaarborgd is.

**Art.24** Gebruikers schrijven zich niet in op "mailing lists" die niet gerelateerd zijn hun professionele activiteiten. Een "mailing list" komt overeen met een inschrijving voor het automatisch en regelmatig bekomen van informatie.

**Art.25** Het gebruik van sociale media door de gebruiker is toegelaten wanneer dit nodig is voor de goede uitoefening van de taak. Het bestuur behoudt zich ten alle tijde en zonder opgave van enig motief het recht voor om het gebruik van sociale media aan banden te leggen, hetzij door een verbod op te leggen aan de gebruikers om nog langer netwerksites te bezoeken, hetzij door een technische ingreep die het onmogelijk maakt om de netwerksites te bezoeken.

**Art.26** Gebruik van (generatieve) AI wordt gelimiteerd tot het delen publiek toegankelijke informatie. Er mogen in geen geval persoonsgegevens of specifieke data van het lokaal bestuur gedeeld worden.

## Verwerken van persoonsgegevens

**Art.27** Deze policy geldt eveneens voor alle gegevens die via de ICT-systemen worden geproduceerd, overgedragen of erin worden opgeslagen.

**Art.28** Wat het verwerken van persoonsgegevens betreft, gedraagt de gebruiker zich conform de 8 basisprincipes van de wet op bescherming van persoonsgegevens:

1) Legitimiteit: Persoonsgegevens dienen op een rechtmatige wijze verwerkt te worden. Dit betekent dat er telkens een rechtsgrond nodig is waarop het bestuur zich kan beroepen. De meest voorkomende rechtsgronden voor een bestuur berusten op een wettelijke of contractuele verplichting, of op een taak van algemeen of vitaal belang. Indien de gebruiker zich hier niet op kan beroepen is toestemming van de burger noodzakelijk.
2) Finaliteit: De verwerking van persoonsgegevens is enkel toegelaten op basis van een duidelijk omschreven doeleinde en mogen niet verder worden verwerkt voor andere doeleinden die daarmee niet verenigbaar zijn.
3) Transparantie: Betrokken burgers moeten steeds geïnformeerd worden over de verwerking van hun persoonsgegevens.
4) Proportionaliteit: Persoonsgegevens die verwerkt worden, moeten in verhouding staan tot de gegevens die nodig zijn voor het doel van de verwerking. (toereikend, ter zake dienend en niet overmatig)
5) Integriteit: Persoonsgegevens dienen bij een verwerking juist te zijn en te blijven. Zo nodig moeten ze worden geactualiseerd.
6) Opslagbeperking: Persoonsgegevens mogen niet langer bewaard worden dan de wettelijke archiveringstermijn of de interne bewaarvoorschriften. Deze voorschriften zijn gebaseerd op het principe dat betrokkenen niet meer identificeerbaar zijn nadat het verwerkingsdoel gerealiseerd is.
7) Veiligheid: Persoonsgegevens dienen beschermd te zijn door nodige technische en organisatorische beveiligingsmaatregelen.

8) Derden: Persoonsgegevens mogen niet uitgewisseld worden met derden, tenzij dit voorzien is in een wettelijke of contractuele rechtshandeling.

**Art.29** Het bestuur en het personeel zijn verantwoordelijk voor de verwerking van persoonsgegevens.

## Verboden

**Art.30** Zonder limitatief te zijn, mag de ICT-infrastructuur van het bestuur nooit (noch beroepsmatig, noch bij persoonlijk gebruik) gebruikt worden voor volgende zaken:

§1 om informatie te verkrijgen, te verwerken, te verspreiden of op te slaan in strijd met de regelgeving, in het bijzonder (niet-limitatieve opsomming):
- de wetgeving op de bescherming van de persoonlijke levenssfeer,
- de wetgeving in het domein van de telecommunicatie
- de wetgeving over de handelspraktijken die betrekking hebben op commerciële communicatie;
- de wetgeving over het auteursrecht en andere intellectuele rechten;
- de wetgeving ter bestrijding van het racisme of informatie die in het algemeen beledigend of lasterlijk is voor andere personen;
- de wetgeving over de bescherming van de goede zeden (informatie die een pornografisch of uitgesproken erotisch karakter heeft);

§2 om acties te ondernemen die de beveiliging van systemen of informatie in het gedrang kunnen brengen, zoals bijvoorbeeld:
- interne en externe systeem- en netwerkbeveiliging omzeilen,
- schadelijke software (bijvoorbeeld programma's besmet met virussen) creëren of op de computers van het bestuur introduceren,
- zich toegang verschaffen tot systemen of informatie waartoe men niet geautoriseerd is;
- toegang tot het netwerk verschaffen aan personen die hiertoe niet geautoriseerd zijn, behoudens in opdracht van het bestuur;
- een valse identiteit aannemen;
- bestanden van andere personeelsleden verwijderen of wijzigen, behoudens expliciete toestemming;
- downloaden, kopiëren en installeren van software zonder toestemming van het bestuur;
- programma's gebruiken in strijd met de licentievoorwaarden;
- de structuur of de configuratie van de ICT-infrastructuur wijzigen zonder toestemming van het bestuur;

§3 om informatie te verkrijgen, te verwerken, te verspreiden of op te slaan die:
- schadelijk kan zijn voor het bestuur of het imago ervan;
- vertrouwelijk is of die wegens de aard ervan redelijkerwijze als vertrouwelijk moet worden beschouwd, tenzij men die informatie in het kader van de toegewezen opdracht moet behandelen en dit niet indruist tegen de regelgeving;
- hinderlijk is voor anderen zoals aan grote groepen van gebruikers ongewenste berichten verspreiden, lasterlijke feiten verspreiden of onware en geringschatte informatie verspreiden;
- aanstootgevend is voor anderen omdat ze tegen de algemeen geldende fatsoenregels indruist;

§4 om deel te nemen aan kansspelen of loterijen;

§5 in het kader van een zelfstandige activiteit van de gebruiker;

§6 voor politieke activiteiten of doeleinden.

**Art.31** Zonder limitatief te zijn, mag de ICT-infrastructuur van het bestuur voor de volgende zaken enkel gebruikt worden als dit gebeurt in functie van de uitvoering van de opdracht van de gebruiker:

- om muziek-, radio- of televisieprogramma's te beluisteren/bekijken via het internet;
- om deel te nemen aan chatrooms of newsgroups;
- voor zaken met winstgevend doel.

## Controle

**Art.32** De algemeen directeur, de leidinggevenden, de ICT-medewerker en de functionaris gegevensbescherming waken over de naleving van dit reglement.

**Art.33** Het bestuur kan het gebruik van internet, e-mail en andere communicatiemiddelen permanent of tijdelijk laten controleren. Dit gebeurt desgevallend met eerbiediging van de regels van de privacy.

**Art.34**

§1 Controle op het communicatiegebruik gebeurt enkel met het oog op:

- het voorkomen van ongeoorloofde of lasterlijke feiten, feiten die strijdig zijn met de goede zeden of die de waardigheid van een andere persoon kunnen schaden;
- de veiligheid en/of de goede technische werking van het ICT-netwerksysteem, met inbegrip van de controle op de kosten die ermee gepaard gaan, alsook de fysieke bescherming van de installaties van het bestuur;
- het te goeder trouw naleven van de regels rond gebruik van ICT-middelen zoals vermeld in onderhavige policy (en als bijlage bij het arbeidsreglement gevoegd).

§2 Het bestuur zal in zijn controle niet verder gaan dan nodig is voor het verwezenlijken van deze doelstellingen. Ze kiest de controlemethode die de geringst mogelijke inmenging in de persoonlijke levenssfeer van de gebruiker tot gevolg heeft.

**Art.35** Gegevens of communicatie waarvan niet uitdrukkelijk is aangegeven dat het gaat om privé-informatie, kunnen op elk moment door de algemeen directeur worden ingekeken.

**Art.36** Privécommunicaties kunnen bij ernstig vermoeden van misbruik of van niet-naleving van de policy gecontroleerd worden op hun aantal, tijdstip en/of hun inhoud in het bijzijn van de betrokken gebruiker.

**Art.37** Het resultaat van de controle zal ter kennis van de gebruiker worden gebracht.

## Sancties

**Art.38** De gebruiker kan aansprakelijk gesteld worden voor alle schade die hij opzettelijk heeft toegebracht aan ICT infrastructuur of die voortvloeit uit het onvoorzichtig omspringen met zijn gebruikersnaam, wachtwoord of andere beveiligingsinformatie.

**Art.39** Het bestuur kan de toegang tot ICT-infrastructuur geheel of gedeeltelijk intrekken bij een overtreding van deze policy of van andere onderrichtingen.

**Art.40** Het bestuur kan te allen tijde de toelating tot privégebruik geheel of gedeeltelijk intrekken.

**Art.41** Andere sancties kunnen worden opgelegd conform het arbeidsreglement.