

BIJLAGE 9. REGLEMENT VOOR HET GEBRUIK VAN ELEKTRONISCHE INFORMATIE- EN COMMUNICATIEMIDDELEN OP HET WERK

1. INLEIDING

Het bestuur gelooft dat elektronische communicatiemiddelen de interne en externe communicatie kunnen verbeteren en kunnen bijdragen tot een efficiënte dienstverlening.

Dit reglement wil het efficiënt en veilig gebruik van deze communicatiemiddelen verzekeren en duidelijke afspraken vastleggen over het gebruik, de controlemaatregelen en de eventuele sancties bij misbruik. Hierbij wordt gestreefd naar een evenwicht tussen de bescherming van de persoonlijke levenssfeer van de gebruikers en de controle die de werkgever uitoefent op het gebruik van werkmateriaal.

De algemeen directeur, de dienst ICT en de veiligheidsconsulent waken over de naleving van dit reglement. Eventuele sancties worden opgelegd overeenkomstig het arbeidsreglement, de rechtspositieregeling en de toepasselijke regelgeving.

2. TOEPASSINGSGEBIED

§1. Dit reglement is van toepassing op het gebruik van elektronische communicatiemiddelen en elektronische informatie en gegevens van het bestuur. Het is eveneens van toepassing wanneer een gebruiker eigen apparatuur combineert met de infrastructuur, accounts of toepassingen van het bestuur.

§2. Dit reglement is van toepassing op alle personeelsleden van de gemeente en het OCMW.

§3. Dit reglement is van toepassing op alle externen die toegang hebben tot de elektronische communicatiemiddelen van de gemeente of het OCMW.

3. DEFINITIES

§1. “Elektronische communicatiemiddelen” omvatten de apparatuur, waaronder computers, laptops, vaste en mobiele telefoons, smartphones en tablets, de interne en externe netwerken, internetverbindingen en de programma’s en toepassingen waarmee gegevens kunnen worden geraadpleegd, verwerkt, opgeslagen of verzonden.

§2. “Elektronische informatie en gegevens” omvatten alle informatie in digitale vorm, zoals e-mail, websites, tekstbestanden, foto’s, video’s, apps en geluidsbestanden.

§3. “Toestel van het bestuur” betekent elk toestel dat door het bestuur ter beschikking wordt gesteld, ongeacht of het toestel aan één gebruiker persoonlijk wordt toegewezen of door meerdere gebruikers wordt gebruikt.

§4. “Privégebruik” betekent elk gebruik dat geen rechtstreeks verband houdt met de uitvoering van de functie of een opdracht van het bestuur. Het gebruik van een toestel van het bestuur voor toegelaten thuiswerk via de eigen internetverbinding is geen privégebruik.

4. ALGEMENE BEPALINGEN

Hardware

§1. Hardware die geen eigendom is van het bestuur mag enkel na uitdrukkelijke toestemming van de dienst ICT worden verbonden met computers, toestellen of het netwerk van het bestuur. Deze opsomming is niet limitatief en omvat onder meer externe harde schijven, USB-sticks, camera’s, smartphones en modems.

§2. De door het bestuur ter beschikking gestelde laptops, smartphones, tablets en andere mobiele toestellen zijn in de eerste plaats bestemd voor professionele doeleinden. Privégebruik is uitdrukkelijk verboden, tenzij de medewerker per persoonlijk toegewezen toestel of abonnement uitdrukkelijk kiest dat hij of zij hiervan ook privégebruik wil maken. Deze keuze wordt uitdrukkelijk vastgelegd in de gebruiksverklaring.

Wanneer de medewerker kiest voor privégebruik, wordt het toepasselijke voordeel alle aard via de loonadministratie verwerkt overeenkomstig de geldende wettelijke forfaits. Indien de medewerker niet kiest voor privégebruik, is privégebruik van het toestel of abonnement niet toegestaan. Deze keuzemogelijkheid geldt niet voor gedeelde toestellen. Gedeelde toestellen mogen uitsluitend voor professionele doeleinden worden gebruikt.

§3. De gebruiker mag de beveiligingsinstellingen, beheersprofielen, toegangsbeperkingen of technische configuraties van een toestel van het bestuur niet wijzigen, uitschakelen of omzeilen.

Software en toepassingen

§1. Software en toepassingen mogen uitsluitend door de dienst ICT of in haar opdracht worden gedownload, geïnstalleerd, geconfigureerd of verwijderd.

§2. Gebruikers krijgen geen beheerdersrechten waarmee zij zelf software of toepassingen kunnen installeren, tenzij de dienst ICT dit om gemotiveerde professionele redenen uitdrukkelijk toestaat.

§3. Niet-legale elektronische documenten, spelprogramma's en niet voor de dienst bestemde software of toepassingen zijn niet toegelaten.

§4. Het kopiëren van software van computers of toestellen van het bestuur is niet toegestaan. De gebruiker kan persoonlijk aansprakelijk worden gesteld voor inbreuken op licentievoorwaarden of intellectuele eigendomsrechten.

Antivirussoftware, beveiliging en beheer

§1. Elk toestel is voorzien van de door het bestuur bepaalde beveiligingssoftware en beheerinstellingen. Het is verboden deze uit te schakelen of te wijzigen.

§2. De dienst ICT treft technische maatregelen om niet-toegelaten gebruik te voorkomen of te beperken. Dit kan onder meer gebeuren door het blokkeren van installatierechten, het gebruik van beheersprofielen, toegangsbeperkingen, filtering en registratie van gebruiksgegevens.

§3. Bij een inbreuk kan de toegang tot het netwerk of het toestel onmiddellijk worden beperkt of ontzegd en kunnen verdere maatregelen of sancties volgen.

5. REGELS VOOR HET GEBRUIK

Toegang, gebruikersnaam en wachtwoord

§1. De algemeen directeur beslist, op vraag van de leidinggevende, wie toegang heeft tot welke communicatiemiddelen en onder welke voorwaarden. Deze toegang is strikt persoonlijk en niet overdraagbaar.

§2. Toegang tot de computerinfrastructuur en de communicatiemiddelen wordt verleend door individuele authenticatie. Het gebruik van een persoonlijke gebruikersnaam en een persoonlijk wachtwoord is verplicht.

§3. Iedere gebruiker is verantwoordelijk voor de handelingen die onder zijn of haar gebruikersidentificatie worden uitgevoerd.

§4. Bij het verlaten van de werkplek moet de gebruiker zich afmelden of het toestel vergrendelen.

Professioneel gebruik en privégebruik

§1. De elektronische communicatiemiddelen, accounts, abonnementen en internetverbindingen die het bestuur ter beschikking stelt, zijn in de eerste plaats bestemd voor de uitvoering van de functie en opdrachten van het bestuur. Het gebruik van een eigen internetverbinding voor toegelaten thuiswerk valt niet onder deze terbeschikkingstelling.

§2. De medewerker kiest per ter beschikking gesteld toestel of abonnement of hij of zij hiervan ook privégebruik wil maken. Deze keuze wordt opgenomen in de gebruiksverklaring. Wanneer de medewerker niet kiest voor privégebruik, is uitsluitend professioneel gebruik toegestaan. Dit geldt ook buiten de arbeidsuren en buiten de gebouwen van het bestuur. Toegelaten thuiswerk met een toestel van het bestuur wordt beschouwd als professioneel gebruik.

§3. Wanneer de medewerker niet heeft gekozen voor privégebruik, is het onder meer niet toegestaan om:

- persoonlijke e-mailaccounts, sociale media, streamingdiensten, online winkels of andere privétoeepassingen te gebruiken op een toestel van het bestuur, behalve wanneer dit noodzakelijk is voor een professionele opdracht;
- privégesprekken te voeren, privéberichten te versturen of privédata te gebruiken via een smartphone, telefoonnummer, simkaart of abonnement van het bestuur;
- persoonlijke bestanden, foto's, video's, muziek, apps of documenten op een toestel of netwerkklocatie van het bestuur te bewaren;
- een toestel van het bestuur door gezinsleden of andere derden te laten gebruiken;
- technische beperkingen of beveiligingsmaatregelen te omzeilen.

§4. Wanneer de medewerker niet heeft gekozen voor privégebruik, is uitzonderlijk en onvoorzien privégebruik in een noodsituatie alleen toegestaan wanneer dit redelijkerwijs noodzakelijk is. De medewerker meldt dit zo spoedig mogelijk aan de leidinggevende. Een dergelijke uitzondering creëert geen blijvend recht op privégebruik.

§5. Wanneer de medewerker kiest voor privégebruik:

- moet dit privégebruik buiten de werkuren gebeuren;
- mag het de goede werking of beveiliging van de systemen, de dienstverlening of de arbeidsprestaties niet verstoren;
- mag dit geen abnormale kosten voor het bestuur veroorzaken;
- mag het toestel niet door gezinsleden of andere derden worden gebruikt;
- mogen privé bestanden lokaal bewaard worden zolang dit de goede werking van het toestel niet in het gedrang brengt;
- blijft het opslaan van privé bestanden op de netwerkklocaties van het bestuur verboden;
- blijven de beveiligingsmaatregelen en overige bepalingen van dit reglement onverkort van toepassing.

§6. Wanneer de medewerker kiest voor privégebruik, wordt het toepasselijke voordeel alle aard via de loonadministratie verwerkt volgens de geldende forfaitaire bedragen. Op basis van het RSZ-inspectieverslag van 9 juni 2026 gaat het om de volgende bedragen:

- smartphone:
 - 5,00 euro per maand voor internet/dataverbruik,
 - 4,00 euro per maand voor gesprekken
 - 3,00 euro per maand voor het toestel, tenzij er sprake is van een eigen toestel;
- laptop: 6,00 euro per maand;
- tablet: 3,00 euro per maand.

Wanneer de wettelijk vastgelegde forfaitaire bedragen wijzigen, worden automatisch de op dat ogenblik geldende bedragen toegepast.

§7. Het feit dat een toestel aan een bepaalde medewerker wordt toegewezen, geeft aan de daarop aanwezige gegevens geen persoonlijk karakter. In het kader van hun functie kunnen bevoegde leidinggevendenden of medewerkers van de dienst ICT toegang nemen tot professionele gegevens, met respect voor de toepasselijke privacyregels.

§8. Professionele bestanden worden opgeslagen op de daarvoor voorziene netwerklocaties of cloudomgevingen en niet uitsluitend lokaal op het toestel.

§9. De dienst ICT kan het gebruik controleren overeenkomstig hoofdstuk 8. Privégebruik dat niet overeenstemt met de keuze in de gebruiksverklaring of dat de voorwaarden van dit reglement overschrijdt, kan aanleiding geven tot het intrekken van het toestel of de toegang, het verhalen van aantoonbare kosten voor zover wettelijk toegestaan en een maatregel of sanctie overeenkomstig het arbeidsreglement, de rechtspositieregeling en de toepasselijke regelgeving.

§10. Het is verboden websites te bezoeken waarvan de inhoud illegaal, pornografisch, discriminerend, gewelddadig, schadelijk of kennelijk onveilig is, tenzij de raadpleging ervan aantoonbaar noodzakelijk is voor de uitvoering van de functie. Verdachte websites, links of downloads worden niet geopend en worden in geval van twijfel gemeld aan de dienst ICT. Het downloaden, installeren of uitvoeren van software, browserextensies of andere programmatuur is uitsluitend toegestaan door of na goedkeuring van de dienst ICT.

Gedeelde toestellen

§1. Het bestuur kan gedeelde computers, laptops, tablets of andere toestellen ter beschikking stellen aan personeelsleden die niet beschikken over een persoonlijk toegewezen toestel. Deze toestellen zijn uitsluitend bestemd voor professionele doeleinden, zoals het raadplegen van de tikklok, het intranet, professionele e-mail of andere toepassingen die nodig zijn voor de uitvoering van de functie.

§2. Privégebruik van gedeelde toestellen is niet toegestaan. Het is onder meer verboden om via deze toestellen privéwebsites, persoonlijke e-mail, sociale media, streamingdiensten, webwinkels of andere niet-werkgerelateerde toepassingen te raadplegen of te gebruiken.

§3. Op gedeelde toestellen is geen keuze voor privégebruik mogelijk en wordt bijgevolg geen gebruiksverklaring inzake privégebruik opgesteld. De overige bepalingen van dit reglement over beveiliging, wachtwoorden, toezicht en controle blijven onverminderd van toepassing.

§4. De gebruiker meldt zich na gebruik steeds af en zorgt ervoor dat persoonlijke toegangsgegevens, documenten of andere informatie niet toegankelijk blijven voor een volgende gebruiker.

Thuiswerk en eigen internetverbinding

§1. Tijdens toegelaten thuiswerk mag een medewerker een toestel van het bestuur verbinden met de eigen beveiligde internetverbinding om professionele taken uit te voeren. Dit wordt beschouwd als professioneel gebruik.

§2. Het bestuur stelt voor thuiswerk geen internetverbinding ter beschikking en betaalt de kosten van de privé-internetverbinding niet terug.

§3. Het gebruik van de eigen internetverbinding verandert niets aan de keuze die de medewerker voor het betrokken toestel of abonnement heeft gemaakt. Wanneer de medewerker niet heeft gekozen voor privégebruik, mogen de apparatuur, accounts, toepassingen en abonnementen van het bestuur ook tijdens thuiswerk uitsluitend voor professionele doeleinden worden gebruikt. Wanneer de medewerker wel heeft gekozen voor privégebruik, gelden de voorwaarden van het onderdeel "Professioneel en privégebruik".

§4. De medewerker zorgt ervoor dat gezinsleden en andere derden het toestel niet gebruiken en neemt redelijke maatregelen om de thuisverbinding en de werkomgeving te beveiligen. De medewerker gebruikt geen onbeveiligde openbare wifi, tenzij via een door de dienst ICT goedgekeurde beveiligde verbinding.

Verantwoordelijkheid van de gebruiker

§1. De ter beschikking gestelde apparatuur moet zorgvuldig worden gebruikt, in goede toestand worden gehouden en mag niet onbeheerd worden achtergelaten. De gebruiker respecteert alle beveiligingsmaatregelen.

§2. Overbodige bestanden worden regelmatig verwijderd en mailboxen worden opgeruimd volgens de interne richtlijnen.

§3. Elke medewerker is verantwoordelijk voor de informatie die hij of zij beheert en raadpleegt. Het gebruik is beperkt tot wat voor de uitvoering van de professionele opdracht noodzakelijk is.

§4. Vertrouwelijke informatie en persoonsgegevens moeten met bijzondere zorg worden behandeld en mogen alleen worden bewaard op goedgekeurde locaties en toestellen.

§5. Verwijderbare media en draagbare toestellen met vertrouwelijke informatie worden beveiligd en volgens de interne richtlijnen vernietigd of gewist.

§6. Elke medewerker handelt in overeenstemming met de regelgeving over privacy, auteursrechten, informatieveiligheid, non-discriminatie en de bescherming van derden.

§7. Elke medewerker houdt bij de verwerking en verspreiding van informatie rekening met de belangen en gevoeligheden van het bestuur, de medewerkers en de betrokken burgers.

6. E-MAIL EN DIGITALE COMMUNICATIE

§1. Het professionele e-mailadres, de mailbox en de digitale communicatiekanalen die het bestuur ter beschikking stelt, zijn uitsluitend bestemd voor professionele doeleinden.

§2. Het feit dat het e-mailadres de persoonlijke naam van de gebruiker bevat, geeft aan de mailbox of de berichten geen persoonlijk karakter.

§3. Privécommunicatie via het professionele e-mailadres, professionele chattoepassingen of andere professionele accounts van het bestuur is niet toegestaan, ook niet wanneer de medewerker voor het betrokken toestel heeft gekozen voor privégebruik.

§4. Alle inkomende en uitgaande e-mail en digitale communicatie kan overeenkomstig de wettelijke regels worden geregistreerd, beveiligd en gecontroleerd.

§5. De kwaliteitsregels, huisstijl, beveiligingsrichtlijnen en afspraken over ondertekening en aansprakelijkheidsbeperking moeten worden nageleefd.

§6. Bijlagen worden uitsluitend met goedgekeurde standaardsoftware aangemaakt en verzonden. Voor grote bestanden worden de door de dienst ICT aangewezen kanalen gebruikt.

§7. De gebruiker blijft waakzaam voor spam, phishing, malware en ongeoorloofde vragen naar informatie en meldt verdachte berichten onmiddellijk volgens de interne procedure.

7. KRUISPUNTBANK EN VERTROUWELIJKE GEGEVENS

Bewaring van vertrouwelijke gegevens

Voor de opslag van gevoelige informatie mag uitsluitend gebruik worden gemaakt van de daarvoor voorziene en beveiligde netwerklocaties en toepassingen.

Consultatie van vertrouwelijke gegevens

§1. Gebruikers van toepassingen van de Kruispuntbank van de Sociale Zekerheid of rijksregister mogen uitsluitend persoonsgegevens raadplegen die noodzakelijk zijn voor de uitvoering van hun functie.

§2. Iedere raadpleging kan worden gelogd en gecontroleerd. Onrechtmatige raadplegingen zijn verboden en kunnen worden gesanctioneerd.

§3. Medewerkers nemen alle maatregelen om het vertrouwelijke karakter van de gegevens te verzekeren en gebruiken deze uitsluitend voor professionele doeleinden en wettelijke verplichtingen.

Mededeling van vertrouwelijke gegevens

§1. Iedereen die betrokken is bij de inzameling, verwerking of uitwisseling van persoonsgegevens is gebonden aan de toepasselijke geheimhoudings- en beveiligingsverplichtingen.

§2. Bij een vraag naar persoonsgegevens controleert de medewerker steeds de identiteit en de bevoegdheid van de aanvrager voordat informatie wordt meegedeeld.

§3. Bij twijfel wordt de informatie niet onmiddellijk vrijgegeven en wordt intern afgestemd met de bevoegde collega, leidinggevende, veiligheidsconsulent of functionaris voor gegevensbescherming.

8. TOEZICHT, CONTROLE EN SANCTIES

§1. Het bestuur respecteert de persoonlijke levenssfeer van de medewerkers. Het kan controles uitvoeren om:

- de goede werking, beveiliging en beschikbaarheid van de apparatuur en systemen te verzekeren;
- de naleving van dit reglement en van de keuze inzake privégebruik zoals vastgelegd in de gebruiksverklaring te controleren;
- misbruik, beveiligingsincidenten, abnormale kosten of overtredingen te onderzoeken.

§2. De controle kan betrekking hebben op gebruiks- en verkeersgegevens, geïnstalleerde software en toepassingen, netwerkverkeer, verbindingen, opslaggebruik, oproep- en datagegevens, beveiligingsmeldingen en andere relevante technische gegevens. De controle gebeurt binnen de wettelijke grenzen, is doelgericht en wordt beperkt tot wat noodzakelijk is.

§3. De dienst ICT mag alle controles uitvoeren die noodzakelijk zijn voor het beheer en de beveiliging van de informatiesystemen, het voorkomen van overbelasting en het opsporen van technische of veiligheidsproblemen.

§4. Controles gebeuren in beginsel op globale of geanonimiseerde wijze. Wanneer afwijkingen, veiligheidsrisico's of aanwijzingen van ongeoorloofd gebruik worden vastgesteld, kan de controle worden verfijnd tot op het niveau van een dienst, toestel of individuele gebruiker, voor zover dit noodzakelijk en wettelijk toegestaan is.

§5. Wanneer een gebruiker de veiligheid of de goede werking van het systeem in gevaar brengt, kan de dienst ICT de toegang onmiddellijk beperken, het toestel blokkeren of innemen en de gebruiker identificeren en contacteren.

§6. Bij vermoedens van ernstig ongeoorloofd gebruik, een misdrijf of een ernstige bedreiging van de belangen van het bestuur kan verdere controle plaatsvinden met het oog op het veiligstellen van gegevens en bewijs, binnen de toepasselijke wettelijke procedure.

§7. In andere gevallen wordt de betrokken medewerker uitgenodigd voor een gesprek voordat een individuele maatregel of sanctie wordt opgelegd. De medewerker krijgt de mogelijkheid om uitleg te geven en kan zich laten bijstaan overeenkomstig de geldende regels.

§8. Niet-naleving van dit reglement kan, afhankelijk van de aard en ernst van de inbreuk, aanleiding geven tot:

- een waarschuwing of formele terechtwijzing;
- het tijdelijk of definitief beperken of intrekken van toegang, accounts, abonnementen of toestellen;
- het terugvorderen van aantoonbare abnormale kosten, voor zover wettelijk toegestaan;
- een tuchtmaatregel, disciplinaire maatregel of andere sanctie overeenkomstig het arbeidsreglement, de rechtspositieregeling en de toepasselijke regelgeving;
- aangifte bij de bevoegde instanties wanneer de feiten mogelijk strafbaar zijn.

9. WACHTWOORDBELEID

§1. Elke gebruiker gebruikt een persoonlijk en geheim wachtwoord en, waar voorzien, multifactorauthenticatie.

§2. Wachtwoorden voldoen aan de technische beveiligingsvereisten die door de dienst ICT worden opgelegd. De gebruiker deelt een wachtwoord of verificatiecode nooit met anderen.

§3. Bij een vermoeden van misbruik, verlies of bekendmaking van een wachtwoord moet de gebruiker het wachtwoord onmiddellijk wijzigen en de dienst ICT verwittigen.

§4. Een gebruiker meldt onmiddellijk wanneer hij of zij toegang heeft tot bestanden, toepassingen of netwerken die niet noodzakelijk zijn voor de functie.

§5. Bij het verlaten van de werkplek wordt het toestel vergrendeld of wordt de gebruiker afgemeld.

§6. Het is verboden wachtwoorden van anderen te achterhalen, te gebruiken of beveiligingsmaatregelen te omzeilen.

§7. Wachtwoorden mogen niet onbeveiligd worden opgeslagen of zichtbaar worden achtergelaten.

10. VERKLARING VAN KENNISNAME

Ik bevestig dat ik dit reglement heb ontvangen en gelezen. Ik begrijp dat de elektronische communicatiemiddelen, accounts, abonnementen en toestellen die het bestuur ter beschikking stelt in de eerste plaats voor professionele doeleinden worden gebruikt. Ik maak per ter beschikking gesteld toestel of abonnement een keuze of ik hiervan ook privégebruik wil maken. Deze keuze wordt vastgelegd in de gebruiksverklaring.

Ik verbind mij ertoe de bepalingen en veiligheidsinstructies nauwkeurig na te leven. Wanneer ik kies voor privégebruik, ben ik ervan op de hoogte dat het toepasselijke voordeel alle aard via de loonadministratie wordt verwerkt volgens de geldende forfaitaire bedragen. Ik ben ervan op de hoogte dat het bestuur controles kan uitvoeren zoals beschreven in dit reglement en dat niet-naleving aanleiding kan geven tot het intrekken van toegangen of toestellen en tot maatregelen of sancties overeenkomstig de toepasselijke regels.

Naam	
Functie	
Datum en plaats	
Keuze privégebruik	Smartphone: ☐ Niet van toepassing voor mijn functie

	☐ Uitsluitend professioneel gebruik - privégebruik is niet toegestaan. ☐ Professioneel en privégebruik - het toepasselijke voordeel alle aard wordt via de loonadministratie verwerkt. ☐ Ik gebruik een eigen toestel ☐ Ik gebruik een toestel van het bestuur PC/laptop: ☐ Uitsluitend professioneel gebruik - privégebruik is niet toegestaan. ☐ Professioneel en privégebruik - het toepasselijke voordeel alle aard wordt via de loonadministratie verwerkt.
Handtekening	