

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

update 2025

Inleiding

De ict-infrastructuur is het geheel van middelen die het bestuur als werkgever aanbiedt aan haar personeelsleden om hun taken efficiënt en naar behoren uit te voeren. Het gaat om onder meer vaste en mobiele telefoons, tablets, vaste computers en laptops, e-mail, intranet, internet, wifi, multifunctionele printers of plotters en diverse randapparatuur, maar ook software en toepassingen. Het bestuur wil met deze moderne middelen de kwaliteit van de dienstverlening en de arbeid verhogen.

Het is belangrijk dat er duidelijke richtlijnen zijn over het gebruik van deze middelen opdat de gebruikers weten wat wel of niet 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. De dienst ict neemt veel maatregelen in het kader van de GDPR en de NIS2 richtlijn. NIS2 is een Europese richtlijn (Network and Information Security Directive 2) die de digitale weerbaarheid van de EU moet versterken door striktere cybersecurity-eisen op te leggen aan essentiële en belangrijke sectoren, zoals onder meer voeding, energievoorziening, gezondheidszorg, financiële diensten en de overheid. De richtlijn is sinds oktober 2024 nationale wetgeving in België en verplicht organisaties tot risicobeheer, incidentrapportage, en het naleven van algemeen aanvaarde beveiligingsprincipes, met mogelijks boetes bij niet-naleving.

Doel van de afspraken

Deze gedragscode bevat aanbevelingen en adviezen over het correct gebruik van de ict-infrastructuur, het netwerk en internet. We verlangen van elke medewerker dat hij voor zijn werk en de communicatie daarrond gebruik maakt van het meest geschikte medium.

Deze gedragscode licht ook de manier toe waarop het bestuur omgaat met het monitoren van de ict-infrastructuur in het algemeen en het registreren, verzamelen en monitoren van tot een persoon herleidbare gegevens over onder andere het e-mail-, internet-, en telefoongebruik.

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

1. Gebruik van telefoon en smartphone

In principe wordt de telefoon enkel gebruikt voor de uitvoering van uw taken. Probeer het gebruik van de telefoon voor privégesprekken tijdens de werkuren zoveel mogelijk te vermijden. Dat geldt ook voor het gebruik van andere communicatie-apps.

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

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

Algemeen

Het gebruik van de ict-infrastructuur is enkel toegestaan voor de uitvoering van je taken. Tijdens de diensturen moeten de personeelsleden zich volledig aan hun functie 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 elk gebruik dat de infrastructuur kan overbelasten of in gevaar brengen.

Het bestuur erkent dat je bij de uitoefening van jouw taak recht hebt op respect voor je persoonlijke levenssfeer en dat je occasioneel privécontacten mag onderhouden, met collega's en met derden buiten het bestuur, maar slechts voor zover dat dit niet storend is voor uw normale werkzaamheden. Het toezichthoudend personeel of de systeembeheerders 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, dat steeds kan beperkt of ingetrokken worden.

Bescherming van netwerk en systeemcapaciteiten

Het gebruik van internet, externe portalen en internetdiensten hebben uiteraard invloed op de beschikbare capaciteit (de bandbreedte en de vrije schijfruimte) van de servers en datalijnen van het bestuur. Vermijd misbruik van ons netwerk en optimaliseer op die manier mee de goede werking en vlotte antwoordtijden.

Paswoord

Het gebruik van een unieke pincode of een uniek paswoord is verplicht voor aanmelding op het netwerk. Jouw gebruikersnaam bepaalt welke rechten je krijgt op het netwerk. Maak gebruik van een pincode en/of paswoord dat minstens 8 respectievelijk 14 karakters lang is, dat grote en kleine letters bevat, en minstens een cijfer en een speciaal karakter (& @ # ! ...). Gebruik zoveel mogelijk een verschillende code of paswoord voor elke toepassing.

Je mag niet werken met een login-id van iemand anders. jouw pincode en/of paswoorden zijn strikt persoonlijk en geheim. Geef jouw paswoord nooit door tenzij aan de systeembeheerder, en dan nog enkel wanneer dat dringend en strikt noodzakelijk is.

Ingeval je voor jouw werk toegang nodig heeft tot de bestanden van iemand anders of tot de mailbox van een collega, doe dan tijdig een aanvraag bij de dienst ict, na overleg met de betrokkene om uitgebreide rechten te krijgen. Soms is het gebruik van een gedeelde mailbox per dienst een betere oplossing.

Vergrendeling van onbeheerde pc's

Indien je jouw computer onbeheerd achterlaat (voor een vergadering, buitendienst, middagpauze,...) dan moet u jouw computer vergrendelen of afmelden. Openstaande logins op de toepassingen moeten na gebruik en zeker tijdens de middagpauze gesloten worden, ter beveiliging tegen misbruik door onbevoegden. Behalve voor sommige baliepc's zal het netwerk dit ook automatisch doen na een tiental minuten van inactiviteit.

Bewaring van toestellen

Laat een laptop, tablet of smartphone nooit zonder toezicht in een auto achter, ook niet uit het zicht of in een kofferbak, zelfs als die afgesloten is. Bij diefstal komt de verzekering in zulke gevallen nooit tussen. Berg ook thuis uw toestel veilig weg.

Software

Niemand mag op eigen houtje eender welke software installeren op zijn computer, laptop, tablet of smartphone van de organisatie. Eender welke software mag alleen door de systeembeheerders of na hun goedkeuring (gedownload en) geïnstalleerd worden. Indien blijkt dat bepaalde toepassingen zonder voorafgaand overleg op toestellen van de werkgever werden geïnstalleerd dan kunnen de systeembeheerders deze programma's verwijderen.

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

De dienst ict heeft een systeem dat helpt bij de installatie van updates en upgrades, zowel van verschillende toepassingen als van Windows zelf. Dat systeem detecteert ook regelmatig of er nieuwe software werd geïnstalleerd op toestellen van het bestuur.

Anti-malware

Elk toestel is voorzien van endpoint protection. Deze beschermt jouw toestel tegen virussen en andere malafide software. Het is strikt verboden om deze software uit te schakelen. Zonder deze software verliest het toestel onmiddellijk elke toegang tot het netwerk. Niemand mag toestellen op ons netwerk koppelen die niet voldoen aan de minimum veiligheidsvereisten die de dienst ict vooropstelt. De goede werking van de endpoint protection software wordt continu gemonitord vanwege het grote belang ervan.

Gebruik van het netwerk

Sla alle door jou aangemaakte bestanden zoveel mogelijk op de gepaste netwerklocaties, Teamsfolders of jouw eigen Onedrive op en niet op jouw eigen harde schijf (C-schijf). Er wordt enkel een reservekopie gemaakt van de folders en bestanden op je eigen harde schijf in de mappen documenten, afbeeldingen en bureaublad. Bij het vervangen van uw pc wordt geen rekening gehouden met de eventueel aanwezige bestanden op je lokale harde schijf.

Ga bewust om met de beschikbare schijfruimte van de bestandsserver. Overbodige en verouderde bestanden moeten regelmatig verwijderd worden. Weinig gebruikte bestanden kunnen periodiek naar de archiefschijf worden verplaatst, eventueel in samenspraak met de systeembeheerders.

Beschikbaarheid van de toepassingen en continuïteit van de dienst

Je zorgt er mee voor dat er geen toepassingen in gebruik zijn waar niemand anders dan jezelf mee overweg kan. Om problemen (met opvolging of permanentie) 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 systeembeheerders in om zulke toepassing dubbel te installeren en zorg er mee voor dat voldoende collega's toegang tot de toepassing hebben. De

gegevens van zulke toepassingen moeten op de netwerkserver staan om gedeeld en gebackupt te kunnen worden, nooit op individuele computers.

Gebruik van externe media, usb-sticks en cd/dvd's

Het gebruik van externe media is toegestaan indien het met de nodige voorzichtigheid gebeurt. Gebruik enkel media die je bekend zijn. Steek nooit zomaar een cd, dvd of usb-stick die ergens gevonden werd in jouw computer, ze kunnen malware bevatten. Alle media dienen voor elk gebruik (ook enkel lezen) gescand te worden op virussen en malware. Dat geldt ook voor bijvoorbeeld externe harde schijven die u door bekenden uitgeleend of ter beschikking worden gesteld. Vraag zo nodig assistentie van de dienst ict.

Beheer van jouw pc

Iedereen is persoonlijk mee verantwoordelijk voor de goede werking van zijn computer. In geval van problemen of vreemde fenomenen, meld je dit zonder uitstel aan de systeembeheerders.

Wanneer je vermoedt dat jouw toestel besmet is door malware, of wanneer je vreemde meldingen (zoals ransomware) op het scherm te zien krijgt, dan moet je onmiddellijk het toestel loskoppelen van het netwerk, desnoods door de netwerkkabel los te maken én wifi uit te schakelen. Nog beter is het om het apparaat direct helemaal uit te schakelen, eventueel trek je ook de stroomdraad los. Bij draagbare toestellen druk je minstens 8 seconden op de aan/uit knop en soms kan het nodig zijn om ook de batterij te verwijderen. Zorg dat je op voorhand weet hoe dat moet. Vraag advies bij de dienst ict.

Indien je 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 jouw computer, dan moet je deze persoon doorverwijzen naar de dienst ict. Ga er niet zelf een gesprek mee aan, geef geen andere contactgegevens door, en klik zeker niet op e-mails of links die deze persoon je zou bezorgen. Doe dit niet op het werk en ook niet thuis. 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.

Locatiebepaling

Ingeval van diefstal of verlies van een mobiel toestel heeft de dienst ict de mogelijkheid om mobiele toestellen van op afstand te wissen of om hun locatie te bepalen. Dat zijn belangrijke mogelijkheden om de schade door verlies van gegevens te beperken of zelfs om het toestel terug te vinden ingeval het gestolen wordt of verloren geraakt. Deze mogelijkheid werkt via de ingebouwde GPS en kan niet worden uitgeschakeld. Deze functie is enkel voorzien op mobiele toestellen die eigendom zijn van gemeente, ocmw of agb Westerlo en dus niet op de toestellen die onze medewerkers privé hebben aangekocht.

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

Algemeen

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 deontologische regels voor ambtenaren 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 jouw opdrachten te vervullen of voor professionele training of studies.

Tijdens de middagpauze mag je voor eigen gebruik surfen, mits je de richtlijnen over de niet toegestane sites naleeft.

Niet toegestaan gebruik

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, tenzij het om professionele nieuwsgroepen gaat.
- het is verboden om bij de uitvoering van uw taken gebruik te maken van private adressen (vb. hotmail of gmail) via webmail. 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).
- Je mag bij het versturen van elektronische gegevens je 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.
- het downloaden en installeren van programma's en te grote bestanden. Indien je van mening bent dat er toch een programma's geïnstalleerd moet worden, dan kan dit enkel met medeweten of onder toezicht van de systeembeheerders.
- het opzetten van allerhande chatsessies met onbekenden. De kans op het oplopen van virussen en op inbraak vergroot hierdoor immers sterk. Vergewis je van de identiteit van alle gasten tijdens Teamsvergaderingen.
- het is verboden via de internettoegang van het bestuur binnen te breken in de eigen sites of in ieder ander netwerk of site. Je mag op geen enkele wijze tussenkomen in de normale werking van het netwerk, noch van enig ander netwerk, zeker niet met de bedoeling de reguliere werking te verstoren.
- Je mag de internettoegang niet gebruiken om op eender welke 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, belediging of inbreuk op iemands integriteit.
- 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

Algemeen

Alle personeelsleden met een mailbox worden aangemoedigd e-mail te gebruiken voor het beter uitvoeren van de hen toevertrouwde taken. E-mail is heel geschikt bij de voorbereiding of de evaluatie van een vergadering en om bijvoorbeeld een agenda of een verslag aan verschillende deelnemers tegelijk te bezorgen. In principe wordt e-mail (voornaam.familienaam@westerlo.be of dienst@westerlo.be) enkel gebruikt voor de uitvoering jouw 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, tenzij bij afwezigheid zoals het bijwonen van een studiedag en andere dienstprestaties op verplaatsing.

Wees constant alert op phishing berichten. Bij elke twijfel vraag je advies aan de dienst ict. Volg de interne opleiding over informatieveiligheid.

Gebruik

Houd er rekening mee 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. Richt je bericht aan bestemmingen in het aan: veld wanneer je van hen actie verwacht. Gebruik het cc: veld voor bestemmingen die je enkel op de hoogte wil brengen van jouw bericht.

Wanneer er veel externe bestemmingen zijn van een bericht, overweeg dan om die in het bcc: veld te vermelden. Zo vermijdt u het ongevraagd en ongewenst doorgeven van e-mailadressen aan een grote groep bestemmingen en mogelijk daaropvolgend misbruik ervan voor bijvoorbeeld spam.

Afwezigheid

Bij een geplande afwezigheid van ten minste twee werkdagen moet je de nodige maatregelen treffen opdat je correspondenten worden verwittigd van jouw afwezigheid, en/of dat de inkomende e-mail automatisch wordt doorgestuurd naar het e-mailadres van de dienst of van een collega van de dienst (in onderling overleg met het diensthoofd). Gebruik hiervoor de out-of-office functie van Outlook en/of stel een gepaste regel in.

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

Je postbus

Te veel berichten en/of te grote bijlagen kunnen het mailsysteem fel belasten en dus vertragen. Je moet dan ook regelmatig onbelangrijke of onbelangrijk geworden berichten uit jouw 'postvak in' te verwijderen. Je kan die berichten archiveren of ze gewoon wissen. Vergeet dan ook niet de map 'verwijderde items' geregeld leeg te maken.

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

Beschikbaarheid van e-mail voor de continuïteit van de dienst

Om in geval van ziekte of vakantie van jezelf of een collega te voorkomen dat de berichten in sommige mailboxen niet behandeld worden, moet je er mee over te waken dat zulke situatie zich niet kan voordoen. Vraag desnoods hulp aan de systeembeheerders 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 extra 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 gebruiken van private adressen (vb. hotmail of gmail) tijdens de uitvoering van je functie. Alle elektronische correspondentie die gebruik maakt van de internettoegang, moet verlopen langs het officiële elektronische adres (dienst@westerlo.be; voornaam.familienaam@westerlo.be).
- eenzelfde e-mail naar een grote hoeveelheid ontvangers versturen. Berichten moeten gericht verstuurd worden in functie van de opdracht die moet worden uitgevoerd. Verstuur geen kettinberichten. De systeembeheerder kan zonodig ingrijpen om de verspreiding van kettinmail te beperken of te verhinderen.
- e-mails van grote omvang versturen (meer dan 12 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 je bij de systeembeheerders terecht.
- het gebruik van e-mail voor commerciële of illegale doeleinden.
- je abonneren op elektronische nieuwsbrieven of magazines indien dit professioneel niet relevant is. Inschrijven in mailing lists indien dit professioneel niet relevant is.

- geen berichten ontvangen waar niet om verzocht is of die niet gewenst zijn. Hiermee worden 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 je je realiseert dat het ontvangen bericht zulk item is, en als dusdanig een onwelkom idee bevat, moet je dit negeren, het bericht definitief verwijderen (shift+delete) en er geen kopieën van bijhouden.

Virusmeldingen

Het is verboden om virusmeldingen naar alle personeelsleden door te sturen. Ontvang je een virusmelding, dan stuur je deze enkel door naar de systeembeheerders 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 je harde schijf zonder medeweten van de systeembeheerder. Andere berichten vragen je 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

Jouw e-mail is in beginsel vertrouwelijk. Dat wil zeggen dat niemand – ook de systeembeheerders of de algemeen directeur niet – kennis neemt van de inhoud van de berichten. Als uitzondering geldt dat er ernstige, aantoonbare aanwijzingen van misbruik bestaan of indien kennisname nodig is in het licht van de algemene veiligheid van de computerinfrastructuur. De headers van de berichten (onderwerpregel, afzender of bestemming, datum van verzending), evenals de omvang van het elektronisch verkeer kunnen doorgaans wel nagegaan worden.

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

Representatie

Als je in jouw communicaties persoonlijke opvattingen uit, dan mag je nooit de indruk wekken dat je spreekt namens het bestuur. Houd 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 van berichten

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

Bestemmingen aangeven

Wees alert wanneer je alle bestemmingen van een bericht in de hoofding 'aan:' wil zetten, omdat daardoor alle bestemmingen het e-mailadres van alle andere bestemmingen kunnen zien. Richt het bericht aan jezelf bij het aan: veld en zet alle andere bestemmingen in het bcc: veld. Zo verspreid je niet ongevraagd de e-mailadressen van de bestemmingen die zo voor spam zouden kunnen misbruikt worden.

5. Agenda

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. Multifunctionele printers

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

Gebruik zoveel mogelijk de optie om beveiligde (uitgestelde) afdrukken te maken, dat gebeurt standaard zo. Jouw printopdracht wordt dan pas afgedrukt wanneer je jouw pincode intikt op de machine (of jouw badge presenteert) 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.

7. Gebruik van sociale media

Je kan via sociale media deelnemen aan gesprekken of discussies over materies waar je 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 je kunt jouw professionele ideeën toetsen aan de realiteit.

Deelname aan sociale media brengt ook een aantal risico's met zich mee, die zowel voor de organisatie als voor jezelf 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 je in eigen naam spreekt of namens de gemeente.

8. Mobiel werken via VPN

Door telewerken vervagen de grenzen tussen privé en werk. In principe gelden bij mobiel of thuis werken dezelfde veiligheidsmaatregelen als wanneer je vanop je werkplek zou werken. Je verbindt er zich toe dat de toegang tot het gemeentelijk netwerk van thuis uit enkel door jezelf zal worden gebruikt en erkent dat je de enige geautoriseerde gebruiker bent. Je mag jouw digitale toegang niet doorgeven aan of raadpleegbaar stellen voor gezinsleden of derden en je onderneemt al het nodige om de veiligheid en de privacy van de geconsulteerde documenten te garanderen. Indien je documenten mee naar huis neemt of van thuis uit raadpleegt, dan tref je de nodige maatregelen om deze informatie te beschermen, zowel thuis als onderweg. Het vertrouwelijke karakter van informatie is immers niet plaatsgebonden.

Het is aangewezen om voor de toegang op afstand enkel gebruik te maken van de toestellen van de organisatie. Die beschouwen we als veiliger vanwege de endpoint protection en die zijn daarop voorzien door middel van een beveiligde VPN verbinding. Andere (privé) apparaten kunnen enkel in beperkte mate toegang krijgen tot bijvoorbeeld webtoepassingen. Voor het werken op afstand is ook het gebruik van MFA vereist (multifactor authentication via de Microsoft authentication app).

Je hebt de plicht om beveiligingsrisico's en incidenten omtrent de aan jou ter beschikking gestelde middelen, documenten en andere informatie (zoals bijvoorbeeld het verlies van data, opslagmedia of toegang door derden), altijd te melden aan de dienst ict en de informatieveiligheidsverantwoordelijke.

Wie op structurele wijze wil thuiswerken, overlegt daarover op voorhand met zijn diensthoofd en formaliseert de nodige afspraken via de personeelsdienst (zie bijlage RPR – telewerk)

9. Gebruik van artificiële intelligentie

Alle personeelsleden worden aangemoedigd om AI te gebruiken voor het beter uitvoeren van de hen toevertrouwde taken. CoPilot kan inspirerend en tijdsbesparend werken, een beperkte AI functionaliteit is voorhanden binnen het Microsoft Office abonnement waarover alle medewerkers beschikken.

Als je AI wil gebruiken:

- maak dan een strikte scheiding tussen jouw professioneel account en je privé account. AI onthoudt je eerdere vragen en interacties en zou zo omgevingen kunnen dooreenhalen.
- bescherm gevoelige informatie. AI werkt meestal op Amerikaanse platformen en dat is problematisch vanwege richtlijnen uit de GDPR (AVG) over persoonsgegevens. Vermijd het gebruik van persoonsgebonden informatie.
- dubbelcheck het resultaat en verrijk het resultaat met eigen inzichten of extra informatie. AI is enkel een statistische toepassing die zelf haar informatie op internet verzamelt (die dus fout kan zijn) maar heeft geen inhoudelijk begrip van de gegenereerde tekst of andere output.
- Wees transparant over het gebruik van AI, vermeld dat je AI hebt gebruikt.

- bekwaam je in het gebruik van AI. De kwaliteit van AI output hangt af van de nauwkeurigheid van de vraagstelling. Volg daar een opleiding voor.
- wees je bewust van de milieu-impact. Het gebruik van AI vereist veel energie en koelwater, gebruik het enkel als het echt meerwaarde biedt.

10. Informatieveiligheid

De gemeente beschikt over heel wat informatie en je 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 (vanwege de GDPR of AVG)

Alle medewerkers zijn verplicht om bij te dragen aan de beveiliging van vertrouwelijke informatie en persoonsgegevens die ze verwerken, aan de integriteit en aan de beschikbaarheid van deze informatie. Deze informatie moet op een gepaste wijze worden behandeld en verwerkt met gepaste discretie. Iedereen waakt erover dat vertrouwelijke informatie niet in verkeerde handen valt en niemand verspreidt deze informatie ongeoorloofd. Iedereen verandert geregeld zijn paswoorden, waar die nog gebruikt worden. Niemand mag informatie gebruiken, ook niet anoniem, die niet nodig is voor de uitvoering van zijn taken. Deze bepalingen blijven ook gelden wanneer medewerkers onze organisatie verlaten.

Zowel aan medewerkers als aan leveranciers kan worden gevraagd om in dit kader een **vertrouwelijkheidsverklaring** te ondertekenen.

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

11. Toezicht en controle

Algemeen

De dienst ict gebruikt verschillende controlesystemen die de werking van de ict-infrastructuur constant monitoren en die een alarm genereren wanneer zich een afwijking voordoet van wat als normaal dagelijks gebruik geldt. Voorbeelden zijn het aanmelden vanuit het buitenland, het onverwacht verzenden van honderden e-mailberichten of het onverklaarbaar opvullen van schijfruimte. Enkel wanneer zulk alarm aanleiding geeft tot verder onderzoek zal de dienst ict de oorzaak van een abnormaal fenomeen proberen te bepalen tot op pc- of mailboxniveau, dus tot bij de individuele gebruiker. In het belang van de algemene veiligheid van het netwerk kunnen de systeembeheerders beslissen om een geïnfecteerde computer of mailbox te isoleren en uit het bedrijfsnetwerk te verwijderen.

In het kader van informatieveiligheid leggen de GDPR en NIS2 ons verplichtingen op vanwege dewelke we het gebruik van interne en externe toepassingen en portalen loggen. We voldoen aan die verplichtingen door het registreren van logons en verwerkingen zodat altijd kan worden nagegaan wie, wanneer en met welk doel toegang had tot welke gegevens.

Er gebeurt ook 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.

In sommige gevallen kan het bestuur, wanneer daar aanleiding toe is en om eventueel ongeoorloofd gebruik van de communicatiemiddelen door de personeelsleden tegen te gaan, andere, statistische controles laten uitvoeren, zoals (niet limitatief):

- aantal telefoongesprekken en hun duurtijd
- de URL's (adressen) van de geraadpleegde websites
- de duur en het ogenblik van de surfsessies
- het aantal en het volume van de uitgaande elektronische mail
- het aantal gemaakte prints of copies

In de mate dat gegevens moeten worden ingekeken, wordt de vertrouwelijkheid door de systeembeheerders gegarandeerd. Na een vaststelling van onrechtmatig gebruik, kunnen deze statistische controles op herhaalde tijdstippen worden uitgevoerd. Enkel wanneer er gegronde aanwijzingen zijn die doen vermoeden dat er misbruik wordt gemaakt van de werkinstrumenten, kan ook de identiteit van de gebruiker worden nagegaan. Dit gebeurt enkel indien er geen andere mogelijkheden zijn om dit misbruik aan te tonen en de betrokkene wordt daarvan vooraf verwittigd.

Het is de werkgever niet toegestaan om kennis te nemen van de inhoud van gesprekken, berichten of afdrukken zonder toestemming van de betrokken medewerker.

Mogelijkheid tot rechtvaardiging van de handelingen

Je wordt op de hoogte gesteld door je diensthoofd of de personeelsdienst wanneer je internetverkeer wordt onderzocht.

Wil je toegang tot een website om professionele redenen waarvan de inhoud niet verenigbaar is met deze gedragscode, neemt je voorhand contact op met je diensthoofd of met de dienst ict.

Uitgangspunten

- De systeembeheerders bewaken de goede werking en het normale gebruik van de ict-infrastructuur. Zij zorgen ook voor de wettelijk verplichte logging.
- Gegevens die tot een persoon herleidbaar zijn, worden niet geregistreerd, verzameld of gecontroleerd, anders dan in deze gedragscode is aangehaald. Hierbij wordt gestreefd naar een maximale bescherming van de privacy van de personeelsleden bij de uitoefening van hun taak.
- Persoonlijke gegevens worden alleen gebruikt voor het doel waarvoor ze verzameld zijn.
- Alle mededelingen die op het intranet gepubliceerd worden, worden verondersteld door iedereen gelezen te zijn.

12. Sancties

Wanneer door het oneigenlijk gebruik van netwerk- en computersystemen schade en/of verlies van gegevens dreigt, zullen de systeembeheerders ingrijpen in die netwerk- en computersystemen teneinde verder onheil te voorkomen. Als zij dat nodig achten, dan kan de netwerk- en internettoegang, eventueel tijdelijk, afgesloten worden.

Onverminderd de eventuele toepassing van de statutair voorziene tuchtregeling kunnen overtredingen van ernstige aard leiden tot het opschorten of beperken van het gebruik van de netwerkdiensten gedurende kortere of langere periode.