2018

E-policy Zonnebeke: Gemeente, OCMW en AGB

CORRECT OMGAAN MET INTERNET, E-MAILS, WACHTWOORDEN EN DRAAGBARE MEDIA

ICT-DIENST I.S.M. WERKGROEP INFORMATIEVEILIGHEID

BESTUUR ZONNEBEKE

Inhoud

Waarom een e-policy?

Deze e-policy regelt het gebruik van internet, e-mail, het netwerk, sociale media, computers en draagbare media door alle werknemers die in opdracht van het bestuur werken.
Internettoegang en e-mail krijg je omdat ze nodig zijn voor je werk en zijn dus eigendom van het bestuur. Van ieder personeelslid wordt verwacht dat er verantwoordelijk, professioneel en integer wordt omgegaan met deze middelen.
Internet, e-mail en sociale media zoals Facebook en Twitter bieden mogelijkheden om het bestuur op een positieve manier voor te stellen. Ons bestuur wenst hiervan deelgenoot te zijn. Evenwel wordt er verwacht van alle personeelsleden dat zij ook hier verantwoord gebruik van maken.
Navermelde regels moeten gelezen worden met in acht name van de geldende wetgevingen (strafwetboek, bescherming van de persoonlijke levenssfeer, …) en de privacyverklaring van de gemeente Zonnebeke.
Alle personeelsleden - ongeacht de aard of duur van de werkrelatie met het bestuur - zullen bij deze hun rechten en plichten kennen en zodoende elk onrechtmatig gebruik van de verschillende systemen kunnen vermijden.

Gebruik toegang tot internet en gebruik van e-mail

Het internet is een communicatiemiddel dat op twee manieren kan gebruikt worden, namelijk privé of beroepsmatig.
Bij gebruik dient iedereen rekening te houden met de noodzaak om de vertrouwelijkheid en de integriteit van de informatie die hij raadpleegt, te respecteren.
Ieder personeelslid is persoonlijk verantwoordelijk voor de inhoud welke hij/zij publiceert op blogs, fora en andere media.
Omwille van veiligheidsredenen dienen de volgende regels te worden toegepast:

<u>Professioneel gebruik</u>

- Indien het nodig blijkt voor de uitvoering van zijn/haar taken krijgt iedere medewerker toegang tot internet.
- Elk gebruik dient gepast te zijn en in overeenstemming met de activiteiten van het personeelslid binnen het bestuur.
- Het is verboden om andere e-mailsystemen (Gmail, Hotmail, Yahoo, …) te gebruiken dan deze die door de instelling ter beschikking worden gesteld of toegestaan zijn.
- Bij afwezigheid of verlof moet het delegeren van toegangsrechten tot de persoonlijke mailbox de uitzondering zijn. Bij voorkeur wordt er gewerkt met gedeelde mailboxen binnen de dienst.
  Een automatische beantwoording moet ingesteld worden, met eventuele doorverwijzing naar een collega of een andere dienst.
- Bij langdurige afwezigheid kan het bevoegde diensthoofd, ingeval van gerechtvaardigde noodzaak, contact op te nemen met de ICT-dienst met het verzoek om toegang te verlenen tot mappen of e-mails.
- Elke e-mail moet voorzien zijn van een handtekening conform de huisstijl die werd opgelegd door de dienst communicatie.
- Elke e-mail moet voorzien zijn van de standaard clausule betreffende de aansprakelijkheid: "*De gemeente Zonnebeke is op geen enkele wijze aansprakelijk voor enige directe of indirecte schade als gevolg van of in verband met het gebruik van deze informatie of documenten. Enkel een officiële brief met de handtekeningen van de burgemeester/ OCMW-voorzitter en de algemeen directeur kan de gemeente verbinden*".

Privégebruik

Voor personeelsleden die over een computer beschikken voor professionele doeleinden is een beperkt gebruik van internet voor privédoeleinden toegestaan à rato van een half uur per dag, tijdens de middagpauze of wanneer het personeelslid is uitgeboekt. En voor zover de bezochte websites niet in strijd zijn met de wet of met huidig reglement. Tijdens de pauzes kan er ook gebruik gemaakt worden van de publieke wifi in de openbare gebouwen.

Beveiliging van de internettoegang

Enkel het bevoegd personeel mag gebruik maken van de toegang tot internetbronnen vanaf de server. Externen die in het gemeentehuis zijn voor werk gerelateerde zaken (vb. vergaderingen) kunnen gebruik maken van de publieke Wifi in het gemeentehuis.
Het bestuur zal de optimale veiligheidsvoorzieningen laten implementeren. Elke poging tot deactivering, wijziging van de configuratie, omzeiling van de beveiligingssystemen is verboden.

Surfen op het internet

Onder surfen op het internet wordt verstaan het raadplegen van websites en het verzamelen van informatie via voorgestelde linken en opzoekingen via gespecialiseerde websites (vb. Google), met als doel relevante informatie in te zamelen.

Bescherming tegen schadelijke websites

- Raadpleging van onprofessionele websites moet vermeden worden
- Ga niet in op pop-upvensters of ongevraagde reclameberichten
- De configuratie van uw browser mag niet gewijzigd worden.
  Enkel de ICT-dienst heeft het recht om de voorwaarden voor het internetgebruik in te stellen
- Deactiveer nooit de beveiligingssoftware (antivirus, firewall, ...)
- De ICT-dienst en informatieveiligheidsconsulent moeten onmiddellijk op de hoogte gesteld worden van ieder vermoeden van abnormaliteit (bijv. een virus) die een negatieve weerslag zou kunnen hebben op de veiligheid van de gegevens
- Het downloaden en installeren van software zonder voorafgaandelijke instemming van de ICT-dienst is niet toegelaten

Deelname aan discussies

- Hieronder wordt verstaan: elke vorm van interactie, zoals online publiceren van informatie, het delen van documenten, het deelnemen aan forums, het gebruik van sociale netwerken, enz….
- Wees u ervan bewust dat alles wat u publiceert voor de hele wereld toegankelijk is
- Respecteer in alle omstandigheden de "nettiquette": gebruik gepaste taal, ….
- Indien social media en netwerking een meerwaarde zijn in de beroepsuitoefening van de gebruiker, is het professioneel gebruik ervan toegelaten, voor zover het redelijk blijft en geen verboden gebruik uitmaakt
- Een officiële mededeling moet steeds gevalideerd worden door de algemeen directeur (en de burgemeester/ OCMW-voorzitter). Deze mededeling moet altijd gebeuren namens het bestuur

Audio en video streaming

- Het is verboden om naar de radio te luisteren of een film te bekijken via het internet.

Gedragscode

Vertrouwelijke Gegevens

Wanneer vertrouwelijke gegevens op elektronische wijze worden ontvangen, dienen de gepaste maatregelen te worden genomen om de vertrouwelijkheid en de integriteit van deze gegevens te waarborgen – met inachtneming van de van kracht zijnde wetgevingen en reglementen.

Bijvoorbeeld: Kruispuntbank van de sociale zekerheid, Rijksregister van natuurlijke personen, Bescherming van persoonsgegevens, enz.

Rechten en plichten

- Ieder personeelslid dat toegang heeft tot internet erkent het recht van de gemeentelijke overheid om controle uit te oefenen op het gebruik ervan - ook wanneer dit gebruik onder de persoonlijke levenssfeer valt.
- Iedereen wordt ervan op de hoogte gesteld dat de toegang tot het internet gefilterd, gecontroleerd, opgeslagen of geanalyseerd kan worden - evenwel in overeenstemming met de terzake geldende wetgeving.
- De gemeentelijke overheid behoudt zich het recht voor om de toegang te blokkeren tot internetsites die volgens de criteria, bepaald hierna onder de titel "gebruiksverbod" als ongepast worden beschouwd.
- Ieder personeelslid is verantwoordelijk voor de ethische aspecten met betrekking tot het gebruik en dient het systeem op een passende wijze te gebruiken.

Gebruiksverbod

Gebruik van internet is in de volgende (of gelijkaardige) gevallen verboden (niet exhaustieve opsomming):

- raadpleging van websites die aanzetten tot betrokkenheid bij illegale, frauduleuze of kwaadwillige activiteiten
- mededeling van gegevens die auteursrechtelijk beschermd zijn
- raadpleging van websites die aanzetten tot laster en eerroof of die informatie met een beledigend, kwetsend en/of bedreigend karakter bevatten
- raadpleging van websites die informatie met een aanstootgevend, obsceen, pornografisch, raciaal of onterend karakter bevatten
- raadpleging van websites die aanzetten tot pesten op grond van geslacht, ras, nationaliteit, fysiek vermogen en/of andere
- raadpleging van websites die aanzetten tot het overtreden van de wet
- mededeling via interactieve sites van feiten die verband houden met:
    - de veiligheid van het land
    - de bescherming van de openbare orde
    - de financiële belangen van de overheid
    - het voorkomen en bestraffen van strafbare feiten
    - het medisch beroepsgeheim
    - de rechten en vrijheden van de burger
    - de eerbiediging van de persoonlijke levenssfeer
    - de voorbereiding van beslissingen, zolang er nog geen eindbeslissing is genomen.

Het is verboden om de intellectuele eigendomsrechten van eender welke partij te schenden. Deze rechten omvatten de reproductierechten, het merkenrecht, het publiciteitsrecht en het privaat recht. Een onevenredig en onredelijk gebruik van de middelen is verboden. Zo is het onder meer verboden om:

- Zware bestanden (video's, spelletjes, muziek, etc. te downloaden
- Systemen te gebruiken die gebruik maken van breedband (streaming video en radio, online spelletjes, etc.)
- Websites te raadplegen die veel systeemcapaciteit opeisen: commerciële websites voor het delen van beelden, websites waarop voortdurend filmpjes worden afgespeeld, etc.)
- De gemeentelijke server te gebruiken voor het bewaren van persoonlijke data.
- Elke aanval op het informaticasysteem en het netwerk is strikt verboden.

Is eveneens niet toegelaten:

- Persoonsgegevens en vertrouwelijke documenten te bewaren in een Cloud-omgeving (Dropbox, Google Docs, …)
- De verspreiding van kettingbrieven
- Het deelnemen aan gokspelen
- De verzending van elektronische post waarbij de identiteit van de verzender wordt verborgen of waarbij men probeert onder een andere naam gegevens te verzenden

- Elk gebruik van het intranet en/of e-mail voor het aankondigen van of het aansporen tot acties die de goede werking van het bestuur kunnen belemmeren.
  Een oproep tot staking is voor alle personeelsleden verboden, ook voor de houders van een vakbondsmandaat.

Publicaties

Publicatie op de website van het bestuur

- Elke publicatie op de eigen website gebeurt door toedoen van de communicatieverantwoordelijke. Hij/zij werkt in dit geval onder de rechtstreekse goedkeuring door de algemeen directeur qua inhoud of bijwerking ervan.
- Indien een personeelslid kennis heeft van welke schade ook die aan de website van de gemeente werd toegebracht, dient hij/zij de ICT-dienst hiervan onmiddellijk op de hoogte te brengen.

Externe publicatie

Elke mededeling van gegevens die:

- rechtstreeks of onrechtstreeks
- in het kader van een professionele of privérelatie
- op eender welke wijze (forum, e-mail, website, blog, sociaal netwerk, …) een invloed heeft op de werking van het bestuur moet worden goedgekeurd door de algemeen directeur.

Wachtwoordbeleid

- Het wachtwoord moet strikt persoonlijk behandeld worden. Bij verlies van het wachtwoord kan de ICT-dienst deze resetten.
- Het is een goede gewoonte om je wachtwoorden voor alle toepassingen geregeld te wijzigen. Personeelsleden worden verplicht om hun wachtwoord elke 3 maanden te wijzigen.
- Het wachtwoord is minstens 8 lang.
- Er moet minstens één hoofdletter, één kleine letter en één cijfer in voorkomen.
- Het mag niet makkelijk te raden zijn aan de hand van uw persoonlijke informatie zoals naam, adres of geboortedatum
- Het wachtwoord mag nergens opgeschreven worden.

Gebruik van draagbare media (laptops, smartphones, USB, …)

- De online-toegang van buiten het bestuur tot de server wordt geregeld via een VPN. Dit is enkel voor toestellen die in beheer van het bestuur zijn.
- Medewerkers die gebruik maken van mobiele toestellen, mobiele media van het bestuur gaan hier zorgvuldig mee om. Er dient een effectieve toegangsbeveiliging toegepast te worden.
- Alle vertrouwelijke informatie die op een draagbare media wordt opgeslagen, moet worden beveiligd tegen elk ongeoorloofd gebruik. In dat opzicht kan elke USB-sleutel met een encryptietool worden vercijferd.
- Medewerkers zijn zelf verantwoordelijk voor smartphones die gebruikt worden voor professionele doeleinden. Deze moeten voorzien worden van een app om alle gegevens vanop afstand te kunnen wissen bij verlies.

Controles en sancties

Toezicht en controle

- Binnen de wettelijke grenzen kan de werkgever controle uitoefenen op gegevens die een personeelslid opslaat, verstuurt of ontvangt binnen het toepassingsgebied van deze richtlijnen. De controle zal gebeuren op een wijze die de inmenging in de persoonlijke levenssfeer tot een minimum beperkt.
- De ICT-dienst en de informatieveiligheidsconsulent mag elke controle uitvoeren die inherent is aan het beheer van het informaticasysteem zelf, om de goede werking van het netwerk te waarborgen of om overbelasting of om veiligheidsproblemen te voorkomen. Deze controles kunnen slechts uitgevoerd worden door een geautoriseerde ICT-deskundige. Alle personeelsleden moeten zich bewust zijn van het bestaan van deze controlemogelijkheid en

van het feit dat alle communicatie die zij via het netwerk uitwisselen, hieraan onderworpen kan worden.
- De werkgever mag het gebruik van de elektronische communicatiemiddelen op een globale wijze controleren. Zo mag een globaal overzicht, eventueel per organisatorische entiteit, van de gedurende een bepaalde periode bezochte websites alsook de frequentie en het volume van de doorgezonden informatie, zonder daarin op enige wijze gegevens over het individueel gebruik op te nemen.
- Indien de ICT-dienst of de informatieveiligheidsconsulent naar aanleiding van zijn/haar controletaken vaststelt dat een of meer gebruikers bewust of onbewust de veiligheid of de goede werking van het systeem in het gedrang brengen, mag hij/zij deze gebruikers onmiddellijk identificeren en, indien nodig, contacteren om de problemen te verhelpen. Hij mag de activiteiten van deze gebruikers, indien noodzakelijk en na verwittiging, ook verder opvolgen om herhaling van het probleem te voorkomen.
- Het gebruik van communicatiemiddelen wordt, buiten het zopas vermelde geval, niet systematisch op individuele wijze gecontroleerd.
- Indien de ICT-dienst of de informatieveiligheidsconsulent ongeoorloofd gebruik vaststelt dat een misdrijf uitmaakt of op ernstige wijze de financiële of economische belangen van de werkgever in het gedrang brengt, kunnen de betrokken gebruikers verder, zonder verwittiging, gecontroleerd worden met het oog op het verzamelen van bewijsstukken.
- In andere gevallen van ongeoorloofd gebruik wordt een waarschuwingsprocedure in acht genomen die hoofdzakelijk tot doel heeft de personeelsleden op de hoogte te brengen van een onregelmatigheid en van het feit dat in de toekomst systematische en individuele controle zal plaatshebben wanneer een nieuwe onregelmatigheid wordt vastgesteld (alarmeringsfase).

Behandeling van incidenten

- Alle gebruikers hebben de verantwoordelijkheid om inbreuken op deze gedragslijn te melden. Incidenten worden gemeld aan de rechtstreeks leidinggevende.
- In afwachting van een definitieve maatregel kan de ICT-dienst of de informatieveiligheidsconsulent voorlopige maatregelen treffen om ernstigere problemen te voorkomen.
- Bij twijfel over de ernst van inbreuk of over de aard van de sanctie kan de rechtstreekse leidinggevende, in alle discretie, het advies van de ICT-dienst of de informatieveiligheidsconsulent inwinnen.
- Bij vaststelling van overtredingen op de gedragslijn kan bij wijze van (een) voorlopige bewarende maatregel(en), minstens één van de volgende stappen ondernomen worden om de veiligheid en integriteit van de systemen en de gegevens te waarborgen:
    - de rechtstreeks leidinggevende van de gebruiker wordt van de situatie op de hoogte gesteld, als dit nog niet gebeurd is;
    - de toegangsrechten van de gebruiker kunnen gedurende het onderzoek opgeschort of beperkt worden (bijvoorbeeld ontzeggen of beperken van de toegang tot het netwerk of de computersystemen, …)

Sancties

Verboden gebruik – zoals omschreven in deze policy – wordt gesanctioneerd afhankelijk van het geval. Mogelijke sancties zijn:

- al dan niet tijdelijke beperking in de toegang tot bepaalde communicatiemiddelen;
- tijdelijk of definitief verbod tot het gebruik van bepaalde communicatiemiddelen;
- indien het misbruik een strafrechtelijk misdrijf uitmaakt, kunnen de betrokkenen voor die feiten tevens gerechtelijk vervolgd worden, ongeacht eventuele schadevorderingen. De werkgever zal meewerken bij het opsporen van dergelijke misdrijven, en zal eventuele gebruikersgegevens en bestanden overmaken aan de gerechtelijke instanties wanneer hierom verzocht wordt;
- sanctioneren volgens de sancties, zoals beschreven in het arbeidsreglement.

Goedkeuring e-policy

- Gemeenteraad dd. 14 mei 2018
- OCMW-raad dd. 11 april 2018, gewijzigd op 22 mei 2018
- Raad van bestuur AGB dd. 11 april 2018, gewijzigd op 16 mei 2018