Bijlage 6 – Afsprakenkader Digitale middelen

Inleiding

Digitalisering en gebruik van digitale middelen is niet meer weg te denken uit onze samenleving en onze organisatie. In dit afsprakenkader geven we richtlijnen over het correct gebruik van de digitale infrastructuur, alle digitale middelen en toepassingen, die binnen het lokaal bestuur Bilzen-Hoeselt ter beschikking worden gesteld.

We onderscheiden 3 thema's:

- Het afsprakenkader ICT
- De gedragscode sociale media
- Het afsprakenkader mobiele toestellen

Het afsprakenkader ICT

Artikel 1 - Doelstellingen

De goede werking van de organisatie is sterk afhankelijk van de vlotte en doeltreffende werking van de Informatie en Communicatie Technologie (ICT) en de manier waarop medewerkers ermee omgaan. Dit afsprakenkader ICT legt regels en richtlijnen vast voor het gebruik van de ICT-middelen van het lokaal bestuur Bilzen-Hoeselt met als doel:

- Een verantwoord gebruik van deze middelen;
- Een optimale werking van de diensten;
- Een afdoende bescherming van de privacy van de gebruikers;
- Een afdoende bescherming van alle personen, wiens persoons- of andere gegevens zijn opgenomen in deze ICT-middelen.

Het afsprakenkader reikt handvaten aan om op een correcte, veilige en effectieve manier om te gaan met de ter beschikking gestelde ICT-middelen.

Dit afsprakenkader geldt voor alle medewerkers, mandatarissen en externen die toegang hebben tot de ICT-middelen van het lokaal bestuur Bilzen-Hoeselt.

Artikel 2 – Welke ICT-middelen worden bedoeld?

Lokaal bestuur Bilzen-Hoeselt biedt haar medewerkers en bepaalde medewerkers van andere organisaties die bij de organisatie een opdracht uitvoeren een aantal informatie-, communicatie- en technologiemiddelen voor de uitoefening van hun taken.

De ICT-middelen kunnen opgesplitst worden in ICT-systemen (netwerk, hardware, software, toegangscodes, ...) en de informatie op ICT-systemen.

Hardware en software zijn bijvoorbeeld (niet limitatief):

- E-mail en internetfaciliteiten;
- Teams en Sharepoint;
- Organisatie- en dienstgebonden applicaties en digitale toepassingen;
- Servers;
- Computers en laptops;
- Smartphones, tablets;
- Badgelezers;
- Printers en multifunctionals;
- USB-sticks;
- Opslagmedia
- ...

De informatie op de ICT-systemen behoort ook tot de ICT-middelen.

Artikel 3 – Hoe omgaan met ICT-middelen?

3.1. Zorgvuldig beheer van ICT-middelen

De medewerker gaat op een voorzichtige en zorgvuldige manier om met de ICT-middelen die gebruikt worden tijdens het werk. Het gebruik van de ICT-middelen is enkel toegestaan voor organisatie-gerelateerde werken en bijkomend enkel op voorwaarde dat het de goede werking en de belangen van de organisatie niet schaadt.

De gebruiker mag niet in onevenredige mate beslag leggen op de informaticamiddelen of de stabiliteit ervan verstoren. Elk gebruik dat indruist tegen de principes van deze richtlijnen of dat in strijd is met de instructies die door het bestuur worden gegeven is niet toegestaan.

De medewerker geeft geen toegang aan derden (vreemd aan het bestuur) tot het netwerk van de organisatie en de bijhorende toepassingen of apparatuur, op welke wijze ook, tenzij een wet of regelgeving hiertoe verplicht. In dat laatste geval blijft de medewerker ertoe gehouden zich voorafgaandelijk ervan te vergewissen dat deze persoon kennis heeft van de richtlijnen.

Daarnaast is de medewerker bereid verantwoording af te leggen over het gebruik van ICT-middelen. De middelen dienen om het algemeen belang na te streven. Bijgevolg worden deze gebruikt met het oog op efficiëntie en effectiviteit.

Onderstaande afspraken gelden voor het omgaan met ICT-middelen:

- Het gebruik van de ICT-middelen is:
  - Steeds in overeenstemming met de doelstellingen;
  - Niet bestemd voor commerciële doeleinden;
  - Niet voor discriminatie, pesten, stalking, spamming,... .

- De medewerker gebruikt de ICT-middelen op een wettelijke manier met respect voor de licentierechten, intellectuele eigendomsrechten, het auteursrecht en de privacy.

- De medewerker neemt contact op met de ICT-dienst om nieuwe software te installeren. Zelf aanpassingen uitvoeren op de computer, software installeren enz. is verboden. De gebruiker mag geen scripts of commando's gebruiken of activiteiten ondernemen, waarvan hij weet of behoort

te weten dat ze de werking en het gebruik van het netwerk op een nadelige wijze kunnen beïnvloeden.

- De medewerker beveiligt de informatie die hij zelf door middel van ICT gebruikt en stuurt nooit informatie door via internet zonder dat specifieke veiligheidsmaatregelen worden genomen;

- De informatie die de medewerker opslaat op het ter beschikking gestelde materiaal blijft eigendom van de organisatie en moet steeds toegankelijk zijn voor de werking van de dienst.

- Als de medewerker definitief de functie verlaat, moet hij alle informatie meedelen die de voortzetting van de dienst mogelijk maakt. Hij zorgt ervoor dat de ICT-middelen die hij mocht gebruiken, terug overhandigd worden aan de organisatie en dat deze na het vertrek nog normaal gebruikt kunnen worden. Medewerkers ondertekenen een document ter staving van de teruggave.

3.2. Telewerken

Het afsprakenkader telewerken is integraal van toepassing.

Daarenboven belichten we hier enkele richtlijnen met betrekking tot het omgaan met de digitale middelen tijdens het telewerken:

- Als de medewerker documenten en materiaal mee op verplaatsing neemt (bv. naar huis), treft hij de nodige maatregelen om die informatie te beschermen, zowel thuis als onderweg.

- Hij respecteert de bestaande afspraken in het bestuur, zowel de algemene afspraken als de afspraken binnen de eigen dienst.

- Het gebruik van alle ICT-apparatuur blijft beperkt tot zakelijke en professionele doeleinden. Het is niet toegelaten om gezinsleden of derden met de apparatuur te laten werken.

- Alle authentificatiemiddelen (paswoorden, Eid, tokens, bankkaarten, ...) mogen nooit samen of in de buurt van een PC of laptop bewaard worden.

- Bij verlies of diefstal zal de verantwoordelijke van de dienst en de IT-verantwoordelijke onmiddellijk verwittigd worden zodat de nodige maatregelen genomen kunnen worden.

- Het bewaren van gevoelige gegevens op de lokale computer of op gegevensdragers moet zoveel mogelijk vermeden worden. Indien dit toch zou gebeuren moet dit steeds op een versleutelde en beveiligde manier gebeuren.

- Het aansluiten van privé-apparatuur of privé-netwerken is niet toegelaten zonder uitdrukkelijke toestemming van de ICT-dienst.

3.3. Behoorlijk e-mail- en internetgebruik

3.3.1 Internet

Elk internetgebruik met een duidelijke link naar het werkkader binnen de werkuren is toegestaan.

Elke vorm van oneigenlijk gebruik van het internet via het netwerk van het lokaal bestuur Bilzen-Hoeselt is verboden. Zonder limitatief te willen opsommen, bedoelen we hier onder andere mee:

- Het opzoeken, downloaden of verspreiden van informatie die een nadelig effect kan hebben op de reputatie of de goede naam van de werkgever, zijn personeelsleden of derden;

- Het trachten in te breken in een computer, database of netwerk;

- Aan kansspelen en online veilingen deelnemen zonder een gewettigd professioneel doel;
- Commerciële activiteiten uitvoeren;

- Erotische, pornografische of obscene websites consulteren;

- Het bezoeken van websites die tegen de grondbeginselen van de democratie en de rechtstaat zijn, die kwetsend of beledigend zijn, die in strijd zijn met de goede zeden of die een gevaar voor verslaving vormen of sites die aanzetten tot discriminatie wegens ras, etnische afkomst, godsdienst, enz..
- ...

3.3.2. E-mail

Wat e-mail betreft, is het gebruik van de officiële e-mailadressen van het bestuur enkel voor professionele doeleinden toegestaan. De uitgewisselde informatie is daarbij ondubbelzinnig gelinkt aan de taken van de medewerker.

In de e-mail wordt geen vertrouwelijke informatie meegedeeld waartoe de medewerker geen bevoegdheid heeft om deze mede te delen.

De medewerker past geldende stijlregels toe. Bij het verzenden van een extern bericht voorziet de medewerker steeds een visuele handtekening. De handtekening wordt automatisch toegevoegd onderaan de werkmail, en bevat minimaal een aantal vermeldingen conform de huisstijl, zoals naam, voornaam, dienst, coördinaten en telefoonnummer.

Bij een afwezigheid langer dan een dag moet de medewerker steeds de “out-of-office reply” vooraf inschakelen. Hij voorziet daarbij een korte afwezigheidsboodschap waarin op een professionele manier de aanvang en het einde van de afwezigheidsperiode vermeld staat. Het e-mailadres en/of telefoonnummer van de collega(‘s) van de betrokken dienst die men kan contacteren tijdens de afwezigheid worden meegedeeld.

Ook bij een onvoorziene afwezigheid stelt de medewerker zelf de "out-of-office-reply" in. Indien de medewerker in de onmogelijkheid verkeert om dit zelf te doen, bv door ziekte, wordt de ICT-dienst op de hoogte gebracht door de medewerker of de rechtstreeks leidinggevende om een afwezigheidsboodschap in te stellen.

Bij een onvoorziene afwezigheid worden in samenspraak met de medewerker afspraken gemaakt met betrekking tot de toegang tot e-mails en de op te volgen dossiers. Enkel bij overmacht wordt een is de rechtstreeks leidinggevende of elke andere door de medewerker aangestelde vertrouwenspersoon ertoe gerechtigd om de mailbox te controleren op inkomende e-mails. Het doel hiervan is de lopende zaken en de continuïteit van de dienstverlening te kunnen garanderen. Deze toegang is evenwel beperkt tot:

- E-mails die verband lijken te houden met lopende dossiers;
- De afwezigheidsperiode waarin correspondenten niet op de hoogte zijn van de afwezigheid.

Er wordt verder gewerkt aan een gedetailleerd afsprakenkader rond toegang tot e-mails in geval van afwezigheid zodat de werknemer goed geïnformeerd is over de te nemen stappen.

Alle e-mailverkeer verloopt via de officiële adressen van het bestuur.

Een e-mail heeft op zich geen bindend karakter. Alle officiële verbintenissen worden gedagtekend en ondertekend door de burgemeester/voorzitter vast bureau en de algemeen directeur.

Het e-mailsysteem is ook niet bedoeld voor het archiveren van belangrijke informatie of het verzenden van persoonsgegevens. Het systematisch doorsturen van werkmail naar persoonlijke mail is ook niet toegestaan.

Als een medewerker e-mailgegevens wil bewaren, moeten die bewaard worden op de juiste locatie op de servers en/of afdrukken en aan het dossier toevoegen.

De medewerker verstuurt geen kettingmails, virussen of valse virusmeldingen. Als hij een virus of valse virusmelding ontvangt, waarschuwt de medewerker de ICT-dienst.

Als de medewerker verdachte spamberichten of andere verdachte berichten in zijn mailbox ontvangt, is hij eveneens verplicht de ICT-dienst te verwittigen.

3.3.3. Filesharing

Het gebruik van onveilige online filesharing diensten die toelaten om veel en/of grote bestanden te delen en op te laden is niet toegestaan. De medewerker moet voorafgaandelijk nagaan bij de dienst ICT welke online filesharing diensten wel veilig en toegelaten zijn of welke tools de medewerker moet gebruiken om bestanden veilig uit te wisselen.

3.4. Omgaan met authenticatiemiddelen

Met authenticatiemiddelen bedoelen we het geheel van wachtwoorden, toegangscodes, persoonlijke aanmeldingsprocedures en -middelen, 2 factor identificatie, …

De medewerker hanteert steeds de authenticatiemiddelen zoals aangereikt door de ICT-dienst of de leverancier.

De medewerker springt voorzichtig om met deze authenticatiemiddelen. Deze zijn geheim, strikt persoonlijk en niet overdraagbaar.

De medewerker respecteert de regels met betrekking tot de digitale identiteit:

- De medewerker verschaft zich enkel toegang tot de ICT-middelen met de hem of haar toegewezen identiteit, tenzij er een gemeenschappelijk account werd aangemaakt;

- De medewerker is persoonlijk aansprakelijk voor alle handelingen die worden uitgevoerd onder zijn identiteit, en geeft authenticatiemiddelen aan niemand door (ook niet aan een rechtstreekse collega, de leidinggevende of aan de dienst ICT);

- Bij een vermoeden dat een persoonlijk wachtwoord of een toegangscode door een ander gekend is, stelt de medewerker dit onmiddellijk en uiterlijk binnen de 24 uur opnieuw in.

De medewerker mag het werkstation niet onbeheerd achterlaten zonder de toegangen tot toepassingen te beveiligen of het werkstation te vergrendelen. Dit geldt ook voor werkstations in vergaderzalen of andere locaties.

Vanaf het moment van uitdiensttreding van de (ex)werknemer worden de authenticatiemiddelen voor de diverse softwarepakketten geblokkeerd.

Bij vermoeden van misbruik kunnen op vraag van de algemeen directeur de authenticatiemiddelen worden geblokkeerd en de toegang worden geweigerd. De dienst ICT neemt op dat ogenblik, mits toestemming van de algemeen directeur, toegang tot alle accounts van de gebruiker.

Artikel 4 – Veiligheidsmaatregelen

Enkel de ICT-dienst of aangestelde derden mogen ICT-middelen installeren, demonteren, verplaatsen of wijzigen. Er mag geen ander materiaal gebruikt worden dan de ICT-middelen die door de ICT-dienst en door de erkende leveranciers ter beschikking werden gesteld.

Enkel software die rechtmatig aangekocht wordt, mag gebruikt worden. Deze moet toegelaten zijn met het oog op het specifieke karakter van de opdrachten en goedgekeurd zijn door de ICT-dienst.

De medewerker dient bestanden op te slaan op Sharepoint.

Als een ICT-middel abnormaal functioneert, dient de medewerker de ICT-dienst onmiddellijk te verwittigen en mag het materiaal niet meer gebruikt worden.

De medewerker mag geen connectie maken van persoonlijke ICT-middelen met het netwerk van het lokaal bestuur, tenzij hij toestemming heeft van de ICT-dienst. Als de medewerker zonder toestemming gebruik maakt van eigen ICT-middelen, zal hij niet ondersteund worden door de ICT-dienst.

De toegang tot bepaalde internetsites kan geblokkeerd worden. Dit kan het geval zijn wanneer hun inhoud onwettig, beledigend of onaangepast zou zijn, vreemd zou zijn aan de activiteiten van het bestuur of omwille van veiligheidsredenen.

Artikel 5 - Controle

5.1. Voorwaarden van controle

De algemeen directeur heeft het recht om controles te laten uitvoeren op het gebruik van internet en e-mail. Daarbij wordt het recht op het privéleven van de medewerkers gerespecteerd. De controle wordt getoetst aan:

- Het finaliteitsbeginsel: een controle is alleen mogelijk voor het nastreven van gerechtvaardigde doelen;
- Het transparantiebeginsel: er wordt open gecommuniceerd over de controles, de doelen en voorwaarden van de controles;
- Het proportionaliteitsbeginsel: de controle en het soort controle moeten in verhouding staan tot het doel van de controle.

Die drie beginselen hebben als doel het evenwicht te houden tussen het recht van het bestuur op controle van werkmiddelen en het recht van de medewerker op zijn privéleven. Om deze controles mogelijk te maken kan het bestuur onder andere de volgende gegevens raadplegen:

- E-mail: het tijdstip, de grootte en de e-mailadressen van afzender en bestemmeling. De gegevens worden gedurende 2 jaar bewaard;
- Internet: het connectietijdstip, de pc die de connectie aanvraagt en het IP-adres van de externe server. De gegevens worden gedurende 1 jaar bewaard.
- Teams-chats: idem als E-mail. Conform het retentiebeleid van Microsoft, worden chats standaard gedurende 2 jaar bewaard.

5.2. Doelen van controle

Controle is alleen mogelijk met de volgende bedoelingen:

- Ongeoorloofde feiten vaststellen en voorkomen. Hiermee wordt bedoeld: lasterlijke feiten, die strijdig zijn met de goede zeden of die de waardigheid van een andere persoon kunnen schaden, zoals:
    - Het kraken van computers, waaronder het op illegale manier inkijken van persoonsgegevens of vertrouwelijke medische bestanden;
    - Het raadplegen van sites die:
        - Zich tegen de grondbeginselen van de democratie en de rechtstaat keren, zoals sites die verband houden met racisme, terrorisme of discriminatie;
        - Anderen kunnen kwetsen of beledigen, zoals sites met racistische of seksistische onderwerpen, pornografisch materiaal of schokkende foto's;
        - Een gevaar voor verslaving vormen zoals goksites en pornografische sites;
        - Iemands privéleven aantasten.

- Bepaalde informatie beschermen. Er zijn uitzonderingen op de principiële openbaarheid van bestuur, omdat bepaalde informatie niet geschikt is om algemeen gedeeld te worden. Een controle is mogelijk als de belangen (opgesomd in het Bestuursdecreet van 7 december 2018) worden geschaad;

- De veiligheid, de performante of de goede technische werking van de IT-systemen van het bestuur verzekeren. Daar hoort de controle op de bijbehorende kosten en de fysieke bescherming van de ICT-omgevingen (installaties) bij;

- Het te goeder trouw naleven van de ICT-richtlijnen;

- De continuïteit van de dienstverlening verzekeren bij overlijden, onvoorziene afwezigheid of vertrek van een medewerker;

- Privacy loggings of controle op de toegang tot bestanden (bv. informatie in authentieke bronnen).

5.3. Algemene controle

De algemeen directeur kan een algemene controle doen op basis van globale gegevens (die geanonimiseerd en op niveau van de organisatie, afdeling of dienst geaggregeerd zijn), zoals:

- Een lijst met oproepnummers, gespreksduur en gesprekskosten;
- Een lijst van de bezochte websites, de frequentie en het volume van de doorgezonden informatie, maar niet de identificatie van de betrokken medewerkers die de sites hebben bezocht;
- Het aantal en het volume van de uitgaande e-mails (niet de binnenkomende berichten), maar niet de identificatie van de betrokken medewerkers die ze hebben verstuurd.
- Analyse van inkomende mails in het kader van anti-spam beleid.

5.4. Individuele controle

Een individuele controle dient steeds in aanwezigheid van een getuige te gebeuren die verbonden is aan het bestuur of door het bestuur werd aangeduid. Een individuele controle is toegestaan voor de volgende doelen en onder de volgende voorwaarden:

- Als uit een algemene controle blijkt dat iemand uit de gecontroleerde groep de ICT-middelen heeft gebruikt in strijd met de richtlijnen. De individuele controle kan in die situatie alleen nadat de algemeen directeur:
    - De betrokkenen heeft ingelicht over het bestaan van een onregelmatigheid;
    - Het personeel op de hoogte heeft gebracht dat de globale gegevens geïndividualiseerd zullen worden als opnieuw een dergelijke onregelmatigheid vastgesteld wordt bij de volgende algemene controle.
- Als uit een algemene controle blijkt dat iemand uit de gecontroleerde groep zich schuldig maakt aan:
    - Ongeoorloofde feiten, laster of feiten die strijdig zijn met de goede zeden of die de waardigheid van een andere persoon kunnen schaden;
    - Het openbaar maken van vertrouwelijke informatie;
    - Feiten die de veiligheid, de performante of de goede technische werking van de ICT-systemen van het bestuur in het gedrang brengen.

In onderstaande gevallen moet de betrokkene niet vooraf worden gewaarschuwd:

- Als een medewerker onvoorzien afwezig is, de dienst heeft verlaten en niet kan worden bereikt of overleden is. In dat geval kan de leidinggevende het werkgerelateerde emailverkeer en de informatie op de opslagmedia raadplegen. Het doel daarvan is de continuïteit van de dienstverlening te garanderen. De raadpleging gebeurt via de informatieveiligheidsconsulent. Die kan dan nagaan welke berichten en informatie werkgerelateerd zijn en dus mogen worden ingezien door de leidinggevende.
- in het kader van een onderzoek bij feiten van geweld, pesterijen en ongewenst seksueel gedrag. Daarbij is de algemeen directeur bevoegd om de verzamelde globale gegevens te individualiseren.

Artikel 6 - Bewaren van persoonlijke gegevens

De persoonlijke gegevens die worden verzameld tijdens een algemene of individuele controle worden bewaard gedurende een periode van maximaal 1 jaar. Medewerkers hebben het recht om hun persoonlijke gegevens (die werden verzameld tijdens de controle) in te kijken en om het bestuur te verzoeken eventueel foute gegevens te wijzigen of te schrappen.

Artikel 7 – Uitdiensttreding / beëindiging van de samenwerking

Voor uitdiensttreding zorgt de vertrekkende medewerker ervoor dat belangrijke professionele mails worden opgeslaan op Sharepoint, doorgestuurd naar een gedeelde mailbox of naar een collega. Dit in het kader van continuïteit van de werking. De medewerker krijgt daarbij ook de kans om privémails te wissen.
Wanneer er een vermoeden is dat de medewerker bedrijfsinformatie, bestanden of belangrijke e-mails ter kwader trouw zou laten verdwijnen of onbruikbaar zou maken (vb. bij ontslag om dringende redenen), kan de algemeen directeur beslissen dat de toegang tot het account onmiddellijk wordt afgesloten. De medewerker krijgt alsnog de mogelijkheid om privé-informatie te verwijderen, maar enkel onder toezicht.

Vanaf het moment van uitdiensttreding heeft de (ex)werknemer geen toegang meer tot de mailbox. De uit dienst tredende werknemer (of indien deze dit nalaat, de ICT-dienst) stelt

een afwezigheidsboodschap in: “Deze mail wordt niet gelezen, want deze medewerker is niet langer in dienst. U kan uw vraag richten tot (mailadres opvolger)”.

Uitzonderlijk kan de algemeen directeur aan de ICT-dienst de opdracht geven om een deel van de inhoud van de mailbox ter beschikking te stellen aan zijn opvolger. Dit kan enkel wanneer aan 3 voorwaarden is voldaan:

- Finaliteit: de inzage van de professionele e-mails moet een gerechtvaardigd doel hebben (vb. het goed functioneren van de organisatie, de continuïteit, …)
- Transparantie: de medewerker wordt geïnformeerd over de mogelijkheid tot inzage in zijn e-mails en de manier waarop dit gebeurd (conform dit afsprakenkader)
- Proportionaliteit: de inzage mag niet verder gaan dan nodig om het doel te bereiken

Een vertrouwenspersoon kan betrokken worden om het goede verloop van de inzage en terbeschikkingsstelling mee te bewaken.

Na maximaal 3 maanden wordt de mailbox afgesloten. De ICT-dienst archiveert deze mailbox en de data erin (geen vernietiging van gegevens).

Artikel 8 - Sancties

De medewerker die bij toepassing van de individualiseringsprocedure verantwoordelijk wordt gesteld voor een onregelmatigheid bij het gebruik van de ICT-middelen, wordt uitgenodigd voor een gesprek vóór enige beslissing of evaluatie die hem individueel kan raken. Deze procedure op tegenspraak zal de medewerker in staat stellen het gebruik van de hem ter beschikking gestelde ICT-middelen te rechtvaardigen.

Naar aanleiding van elke inbreuk op deze richtlijnen kan het bestuur – na verloop van voormelde procedure – de nodige maatregelen treffen. Voor de statutaire medewerkers is dit de tuchtprocedure. Voor de contractuele medewerkers geldt artikel 18 van het arbeidsreglement.

Gedragscode sociale media

Artikel 9 – Doelstelling van de gedragscode

Lokaal bestuur Bilzen-Hoeselt vindt het positief dat medewerkers zowel professioneel als privé actief bezig zijn met sociale media, maar het gebruik ervan brengt ook verantwoordelijkheden met zich mee.

De snelheid waarmee informatie zich via sociale media verspreidt, en het publieke karakter ervan kunnen immers een enorme impact hebben op de organisatie, en dus ook op zijn medewerkers.

Deze gedragscode legt de richtlijnen vast die medewerkers moeten respecteren bij professioneel en persoonlijk gebruik van sociale media.

Artikel 10 – Wat is sociale media?

Sociale media zijn online toepassingen en platformen waar mensen informatie met elkaar kunnen delen. De gebruikers verzorgen zelf de dialoog en interactie met elkaar. Een algoritme neemt op de platformen tevens de rol van een redacteur over. Sociale media gebruiken vaak meerdere internet-toepassingen zoals apps en websites.

Er zijn allerlei verschillende sociale media. Denk aan Facebook, X (Twitter), Instagram, Pinterest, LinkedIn, TikTok, YouTube, Snapchat en WhatsApp. Ook reageren op berichten op nieuwssites, discussiefora, blogs en berichten plaatsen op je eigen blog en zelfs berichten in WhatsApp horen daarbij.

Artikel 11 – Welke plaats hebben sociale media in de organisatie?

Bilzen-Hoeselt kiest ervoor om sociale media op diverse vlakken te benutten. De organisatie is actief op verschillende sociale mediakanalen onder andere om:

- In contact te komen met de doelgroep, potentiële medewerkers en vrijwilligers;
- Activiteiten bekend te maken aan het bredere publiek;
- Kennis en informatie te delen tussen medewerkers en met externe partners;
- …

De officiële communicatie vanuit de organisatie gebeurt alleen via de officiële accounts. De officiële accounts worden beheerd door de dienst MarCom. Ingeval van dienstgebonden accounts / kanalen gebeurt het beheer van het account door de dienst Marcom samen met de betreffende dienst.

Natuurlijk blijven sociale media continu in ontwikkeling. Daarom is het niet uitgesloten dat er in de toekomst kanalen of accounts bijkomen of dat sommige kanalen verdwijnen. De officiële communicatie via deze accounts valt onder de uitsluitende verantwoordelijkheid van de dienst. Deze dienst heeft als enige toegang tot deze accounts.

Alle andere communicatie via sociale media valt onder de uitsluitende verantwoordelijkheid van de betrokken medewerker. Daarbij gaat het om privécommunicatie die (uitsluitend) gebeurt via het persoonlijke sociale media-account van een medewerker (persoonlijke Facebook-pagina op eigen naam).

Artikel 12 - Privé- of professioneel gebruik?

Het onderscheid tussen privé- en professioneel gebruik van sociale media is soms moeilijk te maken, maar het is wel van belang. Zodra volgers en vrienden weten dat iemand voor het lokaal bestuur Bilzen-Hoeselt werkt, kan het immers zijn dat een medewerker daarop aangesproken wordt. De uitlatingen van een medewerker kunnen dan ook gezien worden als uitlatingen van het bestuur. Kortom, alles wat een medewerker post op sociale media, kan een invloed hebben op de professionele reputatie van hemzelf, van het bestuur en van de organisatie.

De hierna opgesomde basisprincipes, do's en don'ts kunnen helpen om de communicatie via sociale media (voor iedereen) veilig te laten verlopen.

Artikel 13 – Basisprincipes

De medewerker moet volgende basisprincipes in het achterhoofd houden bij het gebruik van sociale media (professioneel en privé):

- De medewerker is als enige verantwoordelijk voor de inhoud die hij post op sociale media;
- De medewerker moet er zich van bewust zijn dat hij als medewerker ook ambassadeur is van het bestuur;
- De medewerker let op wat er gepost wordt: posts op sociale media blijven altijd en wereldwijd terug te vinden op het internet (ook al werd de boodschap gewist);
- Wat een medewerker op sociale media deelt met iedereen, is publieke informatie en valt niet onder de bescherming van de privacywetgeving (ook niet wanneer het buiten de werktijden en/of vanuit een persoonlijke account gebeurt).

Artikel 14 – Belangrijkste do's

14.1. Professionele communicatie

- Vragen/reacties op de posts geplaatst op 'gemeentelijke sociale media' worden beantwoord door de dienst Marcom (of bij dienstgebonden social media, door de betreffende dienst) en niet vanuit een eigen persoonlijk account. Laat je niet verleiden om hier in eigen naam zelf een antwoord te formuleren! Je mag natuurlijk een kritisch bericht melden bij de dienst.

- Het delen, liken en retweeten van berichten van 'gemeentelijke sociale media' door medewerkers is wel mogelijk. Onze medewerkers zijn belangrijke 'influencers' voor onze organisatie. En dus is ook hun interactie op dat gebied een meerwaarde voor het bereik.

- De organisatie reageert alleen op berichten die op 'gemeentelijke sociale media' gepost worden. Wat er op andere sociale media geschreven wordt, valt buiten de bevoegdheid van het gemeentebestuur.

- Respecteer auteursrechten en doe waar nodig aan bronvermelding

- Bescherm je privacy en die van anderen. Vraag toestemming om personen te taggen of om foto's van hen te delen. Verspreid nooit foto's die de waardigheid van iemand kunnen aantasten of die een verkeerd of vervormd beeld kunnen geven van de realiteit.

14.2. Persoonlijke communicatie

- Gebruik de privacy-instellingen: selecteer 'vrienden' verstandig, deel niet alles met iedereen, zorg dat taggen zonder voorafgaande controle niet mogelijk is, laat niet eender wie toe om berichten op een tijdlijn te plaatsen, enz.

- Spreek met respect over andere mensen, culturen en waarden;

- Vermeld gerust in de biografie jouw werkplek en welke interesses je hebt, maar maak duidelijk dat de berichten in eigen naam geplaatst worden; gebruik de ik-vorm;

- Gebruik je gezond verstand, wees eerlijk en correct;

- Pas het profiel waar nodig aan en verwijder de verwijzingen naar het lokaal bestuur Bilzen-Hoeselt wanneer je tewerkstelling bij de organisatie eindigt.

- Ga op sociale media niet in discussie over klachten over het gemeentebestuur die geuit worden. Indien er klachten geuit worden kan je hen best doorverwijzen naar de bestaande, "klachten- en meldingsprocedure". Discussies worden zo weinig mogelijk publiekelijk gevoerd. Oeverloze of verhitte discussie hebben geen meerwaarde.

Artikel 15 – Belangrijkste don'ts

15.1. Bij professionele communicatie:

- Maak geen accounts aan op naam van de organisatie zonder toestemming van het bestuur;

- Neem niet deel aan discussiefora zonder goedkeuring van het bestuur;

- Treed niet op als woordvoerder van het bestuur, dat is de taak van de mandatarissen of de dienst MarCom;

- Citeer geen collega's en gebruik hun materiaal niet zonder toestemming;

- Spreek niet slecht over collega- en partnerorganisaties, leden, medewerkers enz.;

- Plaats geen spam;

- Reageer niet onmiddellijk op negatieve uitlatingen over het bestuur, juridische kwesties of crisissituaties, maar licht je leidinggevende of de dienst MarCom in om te bekijken of een reactie aangewezen is en zo ja wie reageert.

15.2. Bij persoonlijke communicatie:

- Verspreid geen interne of vertrouwelijke informatie;

- Verspreid geen lasterlijke berichten over het bestuur of andere berichten die de organisatie kunnen schaden;

- Geef geen kritiek op en spreek niet slecht over collega's, andere medewerkers (vrijwilligers, freelancers), leden, gebruikers, collega- en partnerorganisaties en belanghebbenden;

- Gebruik nooit de naam of het logo van de organisatie in een profielnaam of –foto;

- Treed niet op als woordvoerder van het bestuur.

Artikel 16 – Sancties

Gelet op het belang van een correcte toepassing van deze gedragscode, begrijpen de medewerkers dat elk gebruik van sociale media waarbij deze gedragscode ernstig geschonden wordt, een zware fout kan uitmaken die aanleiding kan geven tot een ontslag om dringende reden voor contractuele medewerkers. Voor statutaire medewerkers kan dit aanleiding geven tot het opstarten van een tuchtprocedure.

Afsprakenkader mobiele toestellen

Dit volgt in een latere fase