**Policy over gebruik van internet, sociale media en e-mail[[1]](#footnote-1)**

Deze policy is van toepassing op alle werknemers die een arbeidsovereenkomst hebben met … *(naam organisatie)*, hierna de werkgever genoemd. Deze policy bepaalt de regels over het gebruik van internet, sociale media en e-mail en de werkgeverscontrole daarop. Hij bevat ook (als bijlage) een gedragscode voor socialemediagebruik binnen en buiten de werktijd.

Deze policy is een onderdeel van de algemeen geldende gedragsregels binnen de organisatie[[2]](#footnote-2). Elke werknemer wordt geacht deze te kennen en na te leven.

**REGELS OVER HET GEBRUIK VAN INTERNET, SOCIALE MEDIA EN E-MAIL**

**1. Algemeen**

De hierna bepaalde regels hebben betrekking op het gebruik dat de werknemers maken van:

* **internet, socialemedia-accounts en e-mailaccounts die de werkgever ter beschikking stelt** (bv. *voornaam.familienaam@organisatienaam.be*)

De werkgever bepaalt autonoom wie hier toegang toe heeft. Hij houdt daarbij o.m. rekening met de relevantie van die toegang voor het uitoefenen van de overeengekomen functie. Hij heeft en behoudt altijd het recht om een werknemer de toegang volledig of gedeeltelijk (bv. de toegang tot bepaalde internetsites of bepaalde sociale media) te ontzeggen. Bijvoorbeeld na overtreding van de hierna bepaalde gebruiksregels of na een functiewijziging.

Alle socialemedia-accounts en e-mailaccounts die de naam van de organisatie dragen, zijn te beschouwen als accounts van de werkgever. Het gaat daarbij zowel om officiële accounts (bv. Facebook-pagina van …*(naam organisatie)*)*,* als omprofessionele deelaccounts (bv. Facebook-pagina van ‘Jan van …(*naam organisatie)’*).   
Werknemers mogen alleen een professionele deelaccount op naam van de organisatie aanmaken met toelating van de werkgever. De werkgever houdt in zijn beoordeling o.m. rekening met de relevantie voor het uitoefenen van de overeengekomen functie.

De hierna bepaalde gebruiksregels hebben betrekking op zowel het professioneel als het privégebruik van deze instrumenten, binnen en buiten de werktijden[[3]](#footnote-3).

* **eigen internet** *(via een 3G-netwerk op de eigen smartphone bv.)***enpersoonlijke socialemedia-accounts en e-mailaccounts** *(gmail of hotmail bv.)*

De hierna bepaalde regels hebben betrekking op het gebruik van deze persoonlijke instrumenten binnen de werktijden.   
Buiten de werktijden is de werknemer uiteraard vrij om zijn persoonlijke instrumenten te gebruiken, zij het dat hij ook dan een zekere verantwoordelijkheid draagt als werknemer van de organisatie. De werkgever verwacht dan ook dat zijn werknemers, zowel binnen als buiten de werktijden, de gedragscode respecteren voor communicatie via sociale media, als bijlage opgenomen bij deze policy.

De hierna bepaalde gebruiksregels gelden ongeacht de drager waarop de werknemer deze instrumenten raadpleegt (pc, smartphone, tablet, …) en ongeacht wie eigenaar is van die drager (de werkgever, de werknemer of een derde).

De **ic-verantwoordelijke** van de organisatie beheert alle informatica- en communicatiemiddelen (ic-middelen) van de werkgever. Dat omvat niet alleen de instrumenten (internet, socialemedia-accounts en e-mailaccounts) maar ook de eventuele dragers (pc’s, laptops, smartphones enz.) en het netwerk dat de werkgever ter beschikking stelt.   
De ic-verantwoordelijke is dan ook het aanspreekpunt m.b.t. licentiebeheer, computer- en netwerkproblemen en -beveiliging. De werknemers zijn verplicht om de ic-verantwoordelijke te verwittigen bij problemen of abnormaliteiten (bv. virussen) die zij ondervinden bij het gebruik en/of de beveiliging van de ic-middelen van de werkgever.

De **communicatieverantwoordelijke** van de organisatie is het aanspreekpunt voor alles wat externe communicatie betreft naar o.a. leden, deelnemers, partnerorganisaties en overheden, en het ruimere publiek. De werknemers kunnen bij deze verantwoordelijke terecht met al hun vragen over externe communicatie. *Bijvoorbeeld bij twijfel over de wenselijkheid van een bepaalde communicatie, met vragen over de juiste toepassing van de gedragscode sociale media of voor de formulering van een reactie op negatieve uitlatingen van derden over de organisatie.*

**2. Gebruik van internet, sociale media en e-mail**

**2.1 professioneel versus privégebruik**

2.1.1 internet

Binnen de werktijden is internetgebruik alleen toegelaten voor professionele doeleinden. Privégebruik van internet is dus alleen toegelaten buiten de werktijden (tijdens pauzes bv.) en op voorwaarde dat:

* de werknemer daarvoor, als hij het ter beschikking heeft, eigen internet gebruikt *(via een 3G-netwerk op de eigen smartphone bv.)*
* de werknemer daarvoor alleen in uitzonderlijke gevallen het internet van de werkgever gebruikt en in dat geval het gebruik beperkt houdt
* het geen hinderpaal vormt voor de goede uitvoering van de arbeidsovereenkomst
* de werknemer daarmee geen inbreuk pleegt op de regels in deze policy, op wettelijke voorschriften of op bepalingen in het arbeidsreglement of in de arbeidsovereenkomst
  + 1. sociale media

Professionele communicatie gebeurt altijd via de socialemedia-accounts van de werkgever. De gedragscode als bijlage van deze policy bepaalt de richtlijnen daarbij.

De socialemedia-accounts van de werkgever zijn uitsluitend bedoeld voor professionele doeleinden. Het is niet toegelaten ze te gebruiken voor persoonlijke doeleinden.

Privégebruik en -communicatie kunnen dus alleen via de persoonlijke socialemedia-accounts van de werknemer4 *(bv. persoonlijke Facebook-pagina op naam van de werknemer)* en is alleen toegelaten buiten de werktijden *(bv. tijdens pauzes of voor de start / na het einde van de werktijden)* op de voorwaarden die gelden voor het privégebruik van internet (zie 2.1.1). De gedragscode als bijlage van deze policy bepaalt de richtlijnen voor deze persoonlijke communicatie zolang de werknemer in dienst is van … *(naam organisatie).*

2.1.3 e-mail

Professionele communicatie gebeurt altijd via de e-mailaccounts van de werkgever.

Die zijn uitsluitend bedoeld voor professionele doeleinden. Het is niet toegelaten ze te gebruiken voor persoonlijke doeleinden.

Privégebruik en -communicatie kunnen dus alleen via de persoonlijke e-mailaccounts van de werknemer4 (gmail, hotmail bv.) en zijn alleen toegelaten buiten de werktijden (bv. tijdens pauzes of voor de start / na het einde van de werkuren ) op de voorwaarden die gelden voor het privégebruik van internet (zie 2.1.1).

**2.2.verboden gebruik**

Het is verboden het internet, de socialemedia-accounts en de e-mailaccounts van de werkgever, binnen en buiten de werktijden, te gebruiken:

* om vertrouwelijke informatie te verspreiden over de werkgever en de organisatie, de werking, leden, gebruikers, medewerkers enz.
* voor het plegen van ongeoorloofde feiten, lasterlijke feiten of feiten die strijdig zijn met de openbare orde of goede zeden
* op zodanige wijze dat dit een aantasting tot gevolg heeft of kan hebben van de waardigheid van een persoon of groep personen, zoals generaliserende of beledigende berichten over ras, nationaliteit, geslacht, handicap, religie of politieke overtuiging van een persoon of een groep van personen
* om informatie of berichten van racistische, gewelddadige of pornografische aard te raadplegen en/of te verspreiden
* om handelingen te stellen die een die een inbreuk vormen op intellectuele eigendomsrechten (bv. auteursrechtelijk beschermde berichten of informatie zonder toestemming verspreiden, software zonder licentie downloaden, piraatmuziekbestanden kopiëren)
* in het kader van professionele activiteiten die losstaan van de arbeidsovereenkomst gesloten met de werkgever
* voor de deelname aan gok- en andere onlinespelen
* voor het raadplegen (zonder toestemming van de werkgever) van websites waarvan de toegang betalend is en registratie vereist is
* op een wijze die de veiligheid en/of de goede werking van de ic-middelen van de werkgever in gevaar zou kunnen brengen (zie verder onder 2.3)
* in het kader van een illegale activiteit, wat die ook moge zijn

Deze opsomming is niet limitatief.

In het kader van bovenstaande verbodsbepalingen heeft de werkgever beslist om de toegang tot volgende websites en sociale media te blokkeren:

*-…*

*-…*

Hij behoudt zich het recht voor ook de toegang te blokkeren tot andere websites of sociale media waarvan hij de inhoud illegaal of ongepast vindt.

Het spreekt vanzelf dat bovenstaande verbodsbepalingen ook gelden als richtlijn bij het gebruik van eigen internet en persoonlijke socialemedia- en e-mailaccounts, gelet op de mogelijke gevolgen van een overtreding voor de organisatie en de werkrelatie.

* 1. **gebruik in functie van veiligheid en goede werking van de ic-middelen**

Omde veiligheid en de goede technische werking van de ic-middelen van de werkgever te kunnen waarborgen, wordt van de werknemer verwacht dat hij:

* het nodige doet om het binnenkomen van mogelijk geïnfecteerde bestanden te vermijden
* het nodige doet om overbelasting van het netwerk te vermijden, o.m. door het downloaden van grote bestanden (mediabestanden in het bijzonder) tot een minimum te beperken
* de standaardbeveiligingsinstellingen niet wijzigt zonder toestemming van de ic-verantwoordelijke
* de login en het paswoord die toegang geven tot de ic-middelen van de organisatie, nooit gebruikt voor andere doeleinden (bv. aanmaak van een account op een website)
* de vermelding van de professionele e-mailadressen van de organisatie op websites en via sociale media tot een minimum beperkt (alleen wanneer dit noodzakelijk is) en in de vermelding te doen als volgt: *voornaam.familienaam (at) organisatienaam.be*
* niet deelneemt aan kettingbrieven, ongeacht hun aard of hun doel

**2.4 afspraken bij afwezigheid of uitdiensttreding**

Om de continuïteit van de werking van onze organisatie te verzekeren, is bij afwezigheid of uitdiensttreding van een werknemer opvolging vereist van de e-mailaccount van de werkgever en van de professionele deelaccounts op sociale media.

Voor de opvolging van de professionele communicatie van de werknemer via de **e-mailaccount van de werkgever** (bv. … *voornaam.familienaam@organisatienaam.be*) gelden volgende regels:

* bij geplande afwezigheid (bv. vakantie of tijdskrediet): de werknemer stelt een automatisch antwoordbericht (out of office) in. Het bericht meldt de afwezigheid, de periode en de collega naar wie de afzender zijn bericht eventueel kan doorsturen.
* bij ongeplande afwezigheid (bv. wegens ziekte): naar keuze van de werknemer stelt de werkgever een automatisch antwoordbericht (out of office) in of krijgt een collega, aangeduid in overleg met de werknemer of een personeelsafgevaardigde, toegang tot de e-mailaccount om de dringend op te volgen professionele e-mails te behandelen
* bij uitdiensttreding: de werkgever stelt een automatisch antwoordbericht in met vermelding van zijn uitdiensttreding en de datum waarop de e-mailaccount verwijderd wordt. Een collega, aangeduid in overleg met de werknemer of een personeelsafgevaardigde, krijgt tot de verwijdering ervan toegang tot de e-mailaccount om de op te volgen professionele e-mails te behandelen

Voor de opvolging van de professionele communicatie van de werknemer via zijn **professionele deelaccount op sociale media** (bv. facebook-pagina van ‘…. *(naam werknemer)* van …*(naam organisatie)’*) gelden volgende regels:

* bij geplande afwezigheid (bv. vakantie of tijdskrediet): de werknemer post een bericht waarin hij zijn afwezigheid en de duur ervan aankondigt, en via welke kanalen de volger / lezer met bv. dringende vragen bij een collega terecht kan
* bij ongeplande afwezigheid (wegens ziekte bv.): de werkgever post een bericht waarin hij de volgers informeert over de afwezigheid van de werknemer, de vermoedelijke periode en via welke kanalen de volger met eventuele dringende vragen e.a. bij een collega terecht kan
* bij uitdiensttreding: de werkgever post een bericht waarin hij de volgers informeert over de uitdiensttreding, de datum waarop de account verwijderd wordt en via welke kanalen de volger bij een collega terecht kan

**REGELS OVER DE CONTROLE OP HET GEBRUIK BINNEN DE WERKTIJD**

**1. Algemeen**

De werkgever kan het (professioneel en persoonlijk) gebruik van internet, sociale media en e-mail via het organisatienetwerk controleren. Hij ziet daarbij toe op de bescherming van de privacy van de werknemers door de wettelijke grenzen en de procedure van cao nr. 81[[4]](#footnote-4) te respecteren.

Concreet voert de werkgever alleen controle uit voor zover die een gerechtvaardigde doelstelling heeft en controleert hij alleen de gegevens die relevant en noodzakelijk zijn om die doelstelling te bereiken, met een zo gering mogelijke inmenging in de persoonlijke levenssfeer van de werknemer.   
De werkgever informeerde vooraf de ondernemingsraad / het comité voor preventie en bescherming op het werk / de vakbondsafvaardiging / de werknemers[[5]](#footnote-5) over zijn voornemen om een controlesysteem te installeren, conform artikel 7 en 9 van cao nr. 81[[6]](#footnote-6). Met de hierna volgende bepalingen informeert de werkgever de werknemers individueel over de installatie van het controlesysteem en alle aspecten daarvan, conform artikel 8 en 9 van cao nr. 81**[[7]](#footnote-7)**.

De werkgever verbindt er zich toe de informatie in dit reglement waar nodig bij te werken en het controlesysteem regelmatig te evalueren in de ondernemingsraad / het comité voor preventie en bescherming op het werk / met de vakbondsafvaardiging[[8]](#footnote-8) om na te gaan of er aanpassingen aan technologische ontwikkelingen mogelijk zijn die de inmenging in de persoonlijke levenssfeer van de werknemers nog meer kunnen beperken.

**2. Controlemodaliteiten**

Vanaf … (*datum[[9]](#footnote-9))* kan de werkgever een systeem installeren voor de controle op het gebruik van internet, sociale media en e-mail via haar netwerk, met volgende kenmerken:

**2.1 controledoelstellingen**

De controle kan uitsluitend gericht zijn op[[10]](#footnote-10):

1. het voorkomen van ongeoorloofde of lasterlijke feiten, feiten die strijdig zijn met de goede zeden of die de waardigheid van een andere persoon kunnen schaden

*Daarbij gaat het in het bijzonder (maar niet uitsluitend) om:*

* + - *het raadplegen van internetsites van pornografische of pedofiele aard*
    - *het raadplegen van internet- en socialenetwerksites die aanzetten tot discriminatie, rassenscheiding, haat of geweld jegens een groep, een gemeenschap of de leden ervan wegens ras, huidskleur, afkomst, religie of nationale of etnische afstamming van deze leden*
    - *het kraken van computers, met o.m. kennisname op ongeoorloofde wijze van vertrouwelijke gegevens (bv. betreffende het personeelsbeheer)*

1. de bescherming van de economische, handels- en financiële belangen van de organisatie die vertrouwelijk zijn, alsook het tegengaan van praktijken die daarmee in strijd zijn.

*Daarbij gaat het in het bijzonder (maar niet uitsluitend) om verspreiding van vertrouwelijke bestanden en de schending van mogelijke vertrouwelijke gegevens.*

1. het waarborgen of herstellen van de veiligheid en/of de goede technische werking van de ic-netwerksystemen van de organisatie, met inbegrip van de controle op de kosten die daarmee gepaard gaan, en de fysieke bescherming van de installaties van de organisatie.

*Daarbij gaat het in het bijzonder om het voorkomen en het detecteren van een overbelasting van het netwerk (door overmatig downloaden bv.) of een verspreiding van virussen, junkmail enz.*

1. na te gaan of de werknemers de regels in deze policy m.b.t. gebruik van internet, sociale media en e-mail te goeder trouw naleven

*Daarbij gaat het in het bijzonder om niet-toegelaten privégebruik, verboden gebruik, gebruik in strijd met de regels rond veiligheid en goede werking van de ic-middelen en gebruik dat niet strookt met de gedragscode sociale media*

* 1. **controleomstandigheden**

De werkgever organiseert de controle permanent *(of)[[11]](#footnote-11)* periodiek, als volgt: …………………………………………………………………………………………………………

*(bv. tijdens bepaalde testperiodes die plaatsvinden op vooraf bepaalde tijdstippen en telkens een maximale duur hebben van …. en/of naar aanleiding van bepaalde gebeurtenissen of omstandigheden op basis waarvan de werkgever oordeelt dat een controle nodig is, zoals een klacht of een vermoeden van misbruik)*

**2.3** **controlemiddelen en -methode**

De werkgever gebruikt volgende controlemiddelen: ……………………………………

*(bv. een specifieke software of andere methode – via het werkstation van de werknemer en/of via de server)*

De inzameling van de elektronische onlinecommunicatiegegevens gebeurt in eerste instantie altijd op globale basis *(men kan bijvoorbeeld een lijst trekken van alle websites en socialenetwerksites die werknemers in een bepaalde periode bezochten, met vermelding van het tijdstip en de duur van de raadpleging, maar zonder een link te leggen met de betrokken werknemer(s)).* Wanneer de werkgever op basis van die globale gegevens een onregelmatigheid vaststelt, kan hij overgaan tot individualisering van de gegevens. Dat houdt in dat hij de verzamelde gegevens verwerkt om de identiteit van de verantwoordelijke werknemer te achterhalen.

Wanneer de werkgever controleert met doelstelling nr. 1, 2 en/of 3 (zoals beschreven onder 2.1), mag hij bij vaststelling van een onregelmatigheid zonder formaliteit overgaan tot individualisering.

Wanneer de werkgever controleert met doelstelling nr. 4 (zoals beschreven onder 2.1), licht hij de werknemers eerst op een duidelijke en begrijpelijke wijze in over het bestaan van de vastgestelde onregelmatigheid en over het feit dat hij de elektronische onlinecommunicatiegegevens zal individualiseren wanneer opnieuw een dergelijke onregelmatigheid wordt vastgesteld. Op basis van de gegevens die hij nadien inzamelt, kan de werkgever vervolgens de werknemer die opnieuw een onregelmatigheid begaat, identificeren. Als de werkgever tot sanctionering wil overgaan, nodigt hij de betrokken werknemer vervolgens uit voor een gesprek[[12]](#footnote-12) om hem te informeren over het verkeerde gebruik van de hem ter beschikking gestelde elektronische onlinecommunicatiemiddelen en zijn voornemen om te sanctioneren (zie verder onder 2.6 sancties). De werknemer krijgt de kans om zijn bezwaren uiteen te zetten en het verkeerde gebruik van internet, sociale media en/of e-mail te rechtvaardigen[[13]](#footnote-13).

Gegevens waarvan het uitsluitend beroepsmatig karakter niet ter discussie staat, kan de werkgever ten slotte zonder verdere procedure individualiseren en raadplegen[[14]](#footnote-14). Ook gegevens die de werknemer publiek maakt via sociale media (doordat hij iedereen toegang geeft tot deze gegevens en de toegang dus niet beperkt via de privacy instellingen) kan de werkgever raadplegen zonder verdere procedure.

* 1. **controlebevoegdheid**

Het toezichthoudend personeel[[15]](#footnote-15) is bevoegd om te beslissen over de wenselijkheid en uitvoering van een controle. Na de uitdrukkelijke beslissing of goedkeuring van het toezichthoudend personeel gebeurt de effectieve controle (globaal + individualisering) conform de bepalingen van deze policy door de ict-verantwoordelijke van de organisatie. Het toezichthoudend personeel en de ict-verantwoordelijke rapporteren over de uitgevoerde controles aan de werkgever (Raad van Bestuur).

Verder is het toezichthoudend personeel ook bevoegd om:

* de gegevens die voortvloeien uit de controle te beoordelen (waar nodig bijgestaan door de ict-verantwoordelijke) om (in een eerste fase, op basis van globale gegevens) eventuele onregelmatigheden vast te stellen en (in een tweede fase) de betrokken werknemer te identificeren
* de gebruiksregels voor internet, sociale media en e-mail, zoals bepaald in deze policy, toe te lichten aan de werknemers
* werknemers te informeren over onregelmatigheden die vastgesteld zijn in het kader van een controle en eventuele voornemens tot beslissing of evaluatie
* sancties op te leggen aan werknemers die de gebruiksregels in deze policy overtreden (zie verder onder 2.6)

**2.5 bewaring en inzage van persoonlijke gegevens**

De werkgever bewaart alle gegevens die verzameld worden tijdens een controle, waaronder eventuele persoonlijke gegevens, voor een maximale duur van ….. *(duur bepalen[[16]](#footnote-16)),* in/op ……………… *(plaats van bewaring bepalen, bv. een centrale server).*

Elke werknemer heeft het recht om bij de werkgever informatie te vragen en te krijgen over de verwerking van zijn persoonlijke gegevens. Op zijn verzoek en binnen de bewaringstermijn kan de werknemer zijn persoonlijke gegevens ook inkijken. De werknemer heeft ten slotte het recht om de persoonlijke gegevens die op hem betrekking hebben te doen verbeteren of te laten verwijderen in de gevallen en op de voorwaarden bepaald door de Privacywet van 8 december 1992 en haar uitvoeringsbesluiten.

* 1. **sancties**

Elke werknemer is persoonlijk verantwoordelijk voor het gebruik dat hij maakt van internet, sociale media en e-mail en de inhoud die hij met deze instrumenten verspreidt. De werknemer is dan ook als enige verantwoordelijk wanneer hij deze instrumenten gebruikt op een wijze die niet strookt met de regels in deze policy.

De werkgever behoudt zich het recht voor om de nodige maatregelen te treffen wanneer een werknemer internet, sociale media en/of e-mail gebruikt op een wijze die niet strookt met de regels in deze policy. Naast de sancties waarin het arbeidsreglement voorziet, kan de werkgever bijvoorbeeld ook de toegang tot internet, sociale media en/of e-mail via het organisatienetwerk tijdelijk of definitief, volledig of gedeeltelijk beperken.

Bij herhaaldelijke inbreuken op de gebruiksregels van deze policy of wanneer het om een ernstige overtreding gaat, behoudt de werkgever zich het recht voor de werknemer te ontslaan om dringende reden.

Ten slotte kan de werkgever de betrokken werknemer ook, conform de wettelijke voorschriften, aansprakelijk stellen als hij met zijn handeling(en) schade berokkend heeft aan de organisatie.

**BIJLAGE:**

**GEDRAGSCODE SOCIALE MEDIA**

Onze organisatie vindt het positief dat haar werknemers zowel professioneel als privé actief bezig zijn met sociale media. Want sociale media zijn ‘in’ en bieden vele mogelijkheden. 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 haar medewerkers.

Daarom deze gedragscode. Ze legt de richtlijnen vast die werknemers van onze organisatie moeten respecteren bij professioneel en persoonlijk gebruik van sociale media. Ze is een onderdeel van de policy m.b.t. gebruik en controle van internet, sociale media en e-mail. Elke werknemer wordt geacht die te kennen en na te leven.

1. **Wat zijn sociale media?**

Sociale media zijn onlinetools en onlineplatformen waarop mensen voortdurend met elkaar in contact staan en zelf de inhoud bepalen. Mensen gebruiken sociale media om hun inzichten en ervaringen, informatie en activiteiten met elkaar te delen. Sociale media kunnen verschillende vormen aannemen. Zo zijn er:

* onlinenetwerken zoals *Facebook en* *LinkedIn*
* microblogs zoals *Twitter*
* websites om bestanden en locaties te delen *zoals YouTube, Flickr, Slideshare en Foursquare*
* blogs

1. **Welke plaats hebben sociale media in onze organisatie?**

Onze organisatie kiest ervoor sociale media op diverse vlakken te benutten. We zijn actief op verschillende socialemediakanalen onder andere om:

* in contact te komen met de doelgroep, potentiële werknemers en vrijwilligers
* activiteiten bekend te maken aan het bredere publiek
* kennis en informatie te delen tussen werknemers en met externe partners
* …

De **officiële communicatie** vanuit onze organisatie gebeurt alleen via de officiële accounts. Op dit ogenblik heeft onze organisatie volgende officiële accounts:

* *…*
* *…*

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 communicatieverantwoordelijke. Hij heeft als enige toegang tot de accounts.

Alle andere communicatie via sociale media valt onder de uitsluitende verantwoordelijkheid van de betrokken werknemer. Daarbij gaat het om:

* **andere professionele (maar niet officiële) communicatie** die gebeurt via de professionele deelaccount van de werknemers (bv. Facebook-pagina van ‘…. *(naam werknemer)* van …*(naam organisatie)’*)
* **privécommunicatie** die (uitsluitend) gebeurt via de persoonlijke socialemedia-account van een werknemer (persoonlijke Facebook-pagina op eigen naam bv.)

1. **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 je voor onze organisatie werkt, kan het immers zijn dat je daarop aangesproken wordt. Je uitlatingen kunnen dan ook gezien worden als uitlatingen van onze organisatie. Kortom, alles wat je post op sociale media kan een invloed hebben op de professionele reputatie van jezelf en van de organisatie. De hierna opgesomde basisprincipes, do’s en don’ts helpen je om de communicatie via sociale media (voor iedereen) veilig te laten verlopen.

1. **Basisprincipes**

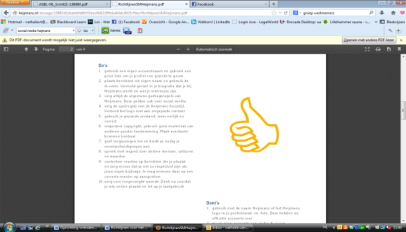
Als werknemer van onze organisatie vragen wij om volgende basisprincipes in het achterhoofd te houden bij het gebruik van sociale media (professioneel en privé):

* je bent als enige verantwoordelijk voor de inhoud die je post op sociale media
* realiseer je dat je als werknemer ook ambassadeur bent van onze organisatie
* let op wat je zegt: wat je post op sociale media blijft altijd en wereldwijd terug te vinden op het internet (ook al heb je de boodschap gewist)
* wat je 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)

1. **Belangrijkste do’s**

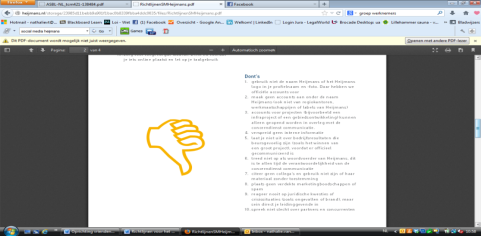
 **bij professionele communicatie:**

* volg ook op sociale media altijd de algemene gedragsregels van de organisatie
* volg de spelregels van de huisstijl van de organisatie
* gebruik een stijlvolle foto om je profiel een gezicht te geven
* beveilig je account door een veilig paswoord
* verbind het logo van de organisatie niet aan ongepaste inhoud
* gebruik sociale media niet alleen voor informatiedeling maar ook voor interactie en dialoog
* participeer en discussieer mee op sociale netwerken over de laatste ontwikkelingen in je vakgebied
* denk na voor je iets online plaatst: zorg voor toegevoegde waarde, wees positief en let op je taalgebruik
* respecteer copyright, gebruik geen materiaal van anderen zonder toestemming, maak eventuele bronnen kenbaar
* geef vergissingen toe en bied zo nodig je excuses aan
* gebruik je privacy-instellingen: selecteer je ‘vrienden’ verstandig, deel niet alles met iedereen, laat je niet taggen zonder voorafgaande controle, laat niet eender wie toe om berichten op je tijdlijn te plaatsen, enz.
* respecteer de privacy van anderen
* spreek met respect over andere mensen, culturen en waarden
* gebruik je gezond verstand, wees eerlijk en correct
* contacteer de communicatieverantwoordelijke bij twijfel of iets past in de professionele communicatie die je als werknemer van onze organisatie wilt voeren, of bij twijfel over de conformiteit van een communicatie met de richtlijnen in deze gedragscode
* kijk de bron en de inhoud van informatie altijd goed na op betrouwbaarheid, integriteit en correctheid voor je die deelt met anderen

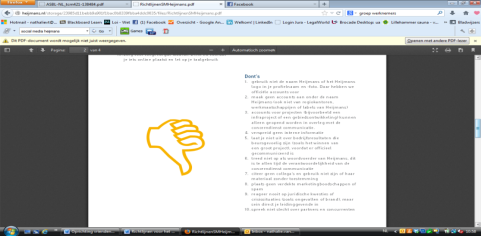
**bij persoonlijke communicatie:**

* gebruik je privacy-instellingen: selecteer je ‘vrienden’ verstandig, deel niet alles met iedereen, laat je niet taggen zonder voorafgaande controle, laat niet eender wie toe om berichten op je tijdlijn te plaatsen, enz.
* spreek met respect over andere mensen, culturen en waarden
* vermeld gerust in je biografie waar je werkt en wat je interesses zijn, maar maak duidelijk dat je je berichten in eigen naam plaatst. Gebruik de ik-vorm
* gebruik je gezond verstand, wees eerlijk en correct
* pas je profiel waar nodig aan en verwijder de verwijzingen naar onze organisatie wanneer je niet langer in dienst bent

1. **Belangrijkste don’ts**

**bij professionele communicatie:**

* maak geen accounts aan op naam van de organisatie zonder toestemming van de werkgever
* neem niet deel aan discussiefora zonder goedkeuring van de werkgever
* treed niet op als woordvoerder van de organisatie, dat is de taak van de communicatieverantwoordelijke
* 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 de organisatie, juridische kwesties of crisissituaties, maar licht je leidinggevende of de communicatieverantwoordelijke in om te bekijken of een reactie aangewezen is en zo ja wie hoe reageert
* maak je niet schuldig aan verboden gebruik (zie policy, 2.2)

**bij persoonlijke communicatie:**

* verspreid geen interne of vertrouwelijke informatie
* verspreid geen lasterlijke berichten over de organisatie 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 je profielnaam of –foto
* treed niet op als woordvoerder van je werkgever
* maak je niet schuldig aan verboden socialemediagebruik (zie policy, 2.2)

**ONTVANGSTBEWIJS**

Ik, ondergetekende: …………….. *(naam werknemer)* heb een exemplaar gekregen van de policy m.b.t. gebruik en controle van internet, sociale media en e-mail, inclusief de ‘gedragscode sociale media’ van ….. *(naam organisatie)*

Gedaan te ………………., op ……………..

Handtekening,

1. Dit is een voorbeeld van policy. Contacteer ons gerust voor een policy op maat van uw organisatie. [↑](#footnote-ref-1)
2. Wij raden u aan om deze policy als bijlage toe te voegen aan uw arbeidsreglement. Daarvoor volgt u de bijzondere wijzigingsprocedure die geldt voor het arbeidsreglement. [↑](#footnote-ref-2)
3. De regels in deze policy beperken zich weliswaar tot het gebruik dat plaatsvindt op de werkplaats. Afspraken over de toegang en het gebruik buiten de werkplaats (thuis of andere locatie) maakt u met elke werknemer afzonderlijk, bv. in een bijlage aan de arbeidsovereenkomst over telewerk. [↑](#footnote-ref-3)
4. Cao nr. 81 tot bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische online-communicatiegegevens van 26 april 2002. [↑](#footnote-ref-4)
5. Schrappen wat niet past. [↑](#footnote-ref-5)
6. Contacteer ons gerust voor bijkomende informatie. [↑](#footnote-ref-6)
7. U geeft deze informatie aan de werknemers uiterlijk wanneer u het controlesysteem installeert. [↑](#footnote-ref-7)
8. Schrappen wat niet past. [↑](#footnote-ref-8)
9. D.i. de datum waarop de policy in werking treedt (cf. inwerkingtreding in het kader van de bijzondere wijzigingsprocedure voor het arbeidsreglement) of een latere datum. [↑](#footnote-ref-9)
10. U kunt de hier opgesomde gerechtvaardigde doelstellingen volledig overnemen of een keuze maken voor een of meer doelstellingen. Andere dan de hier opgesomde doelstellingen zijn niet geoorloofd. Wel kunt u in de toelichting (schuine tekst) de doelstelling verduidelijken op maat van uw organisatie. [↑](#footnote-ref-10)
11. Gelieve een keuze te maken. Let wel: u moet de keuze voor een permanente controle kunnen verantwoorden (relevantie en noodzakelijkheid) in het licht van de vooropgestelde doelstelling(en). [↑](#footnote-ref-11)
12. Tenzij de arbeidsovereenkomst van de werknemer geschorst is. [↑](#footnote-ref-12)
13. Het gesprek moet plaatsvinden voor beslissing of evaluatie die de werknemer individueel kan raken. [↑](#footnote-ref-13)
14. Aangezien deze policy elk privégebruik van de e-mailaccount en de sociale media accounts van de werkgever verbiedt, betekent dit in elk geval dat de werkgever in principe als louter beroepsmatig mag beschouwen en dus vrij mag raadplegen (mits hij daarvoor een gerechtvaardigde doelstelling heeft en het raadplegen relevant en noodzakelijk is om die doelstelling te bereiken):

    alle verzonden e-mails via de account van de werkgever (let wel: omdat de werknemer niet volledig in de hand heeft welke e-mails hij van derden krijgt, is wel enige voorzichtigheid geboden bij het raadplegen van de inkomende mails (best laten beoordelen door neutraal tussenpersoon o.b.v. het onderwerp).

    alle communicatie via de socialemedia-account van de werkgever [↑](#footnote-ref-14)
15. Het arbeidsreglement bepaalt wie daarmee bedoeld wordt. [↑](#footnote-ref-15)
16. Cao nr. 81 bepaalt geen maximumduur, maar stelt alleen dat die niet langer mag zijn dan noodzakelijk voor de gerechtvaardigde doelstelling. In het kader van de Europese Richtlijn (waarvan de privacywet en cao nr. 81 de nationale omzetting zijn) schuift de ‘Data protection Working Party’ een maximumduur van 3 maanden naar voor. [↑](#footnote-ref-16)