ARBEIDSREGLEMENT VOOR HET PERSONEEL VAN HET OCMW

(vastgesteld door de OCMW-raad in zitting van 30 oktober 2003, gewijzigd op 05 oktober 2017 en 31 januari 2022.)

I. ALGEMEENHEDEN

Artikel 1 - Toepassingsgebied

Dit arbeidsreglement is van toepassing op alle personeelsleden van het OCMW Mesen, zowel de statutairen, de tijdelijk statutairen, de contractuelen, de gesubsidieerde contractuelen, de personeelsleden op proef en de stagiairen.

Dit arbeidsreglement is van toepassing voor zover het niet in tegenstrijd is of zal zijn met de algemene, wettelijke, reglementaire en administratieve bepalingen die steeds voorrang hebben (o.m. het administratief statuut en het reglement voor de contractuelen).

De bijlagen maken integraal deel uit van het arbeidsreglement.

Artikel 2 - Naleving van de bepalingen

Aan elk personeelslid wordt een exemplaar van het arbeidsreglement overgemaakt, ook van elke wijziging, tegen handtekening voor ontvangst. Het OCMW en personeel zijn dan ook gebonden aan de bepalingen die in het arbeidsreglement voorkomen en zijn ertoe gehouden ze na te leven.

Artikel 3 - Mogelijke individuele afwijkingen

Alleen voor de contractuele personeelsleden kan worden afgeweken van het arbeidsreglement. Deze afwijking moet, na overleg, schriftelijk vastgelegd worden in een overeenkomst tussen werkgever en personeelslid.

Artikel 4 - Onthaal

Bij de indiensttreding zal een daartoe door de secretaris aangeduid ambtenaar het nieuwe personeelslid in zijn werkkring inleiden. Het nieuwe personeelslid krijgt een overzicht van zijn rechten, verplichtingen, verlofregelingen alsmede de bepalingen van het geldelijk en administratief statuut (of reglement van de contractuelen), het arbeidsreglement en de nodige veiligheidsvoorschriften welke van toepassing zijn tijdens de uitoefening van de functie.

II. AARD VAN HET OVEREENGEKOMEN WERK

Artikel 5

Ieder personeelslid moet de arbeid verrichten waarvoor hij/zij werd aangeworven.
Hij mag niet weigeren tijdelijk andere, bij zijn lichamelijke en verstandelijke geschiktheid passende, arbeid te verrichten wanneer de werkgever daarvoor beroep op hem doet voor de goede gang van zaken binnen het OCMW (zoals vb. bij afwezigheid van een ander personeelslid, bij dringend werk, bij technische stoornis, enz.). Voor dat vervangingswerk zal geen lager loon worden betaald dan het loon dat het personeelslid voordien verdiende.

Artikel 6

Gedurende een eventuele opzeggingstermijn, om het even of de opzegging door het OCMW of door het personeelslid werd gegeven, kan het OCMW het personeelslid in een ander lokaal doen werken en/of zelfs een andere arbeid opleggen mits de bepalingen inzake geschiktheden en inzake loon, waarvan sprake in artikel 4, in acht worden genomen.

III. WERKPLAATS

Artikel 7

Het OCMW werft personeelsleden aan voor een bepaalde functie, niet voor een bepaalde dienst. Een mutatie van dienst is steeds mogelijk in overleg met het personeelslid.

IV. ARBEIDSTIJD

Artikel 8 - Arbeidstijd

Elk personeelslid moet aanwezig zijn op de plaats waar de arbeid moet worden verricht, op het vastgestelde beginuur en er blijven tot het einduur.

Aanvang en einde van de gewone arbeidsdag, alsook tijdstip en duur van de onderbrekingen worden volgens de uurroosters in bijlage 1 geregeld. Zij kunnen volgens de noodwendigheid van de dienst gewijzigd worden volgens wettelijke procedure.

Elk te laat komen op het werk belemmert de goede werking van de dienst en kan aanleiding geven tot sancties. Alleen in gevallen van bewezen overmacht kan hiervan afgeweken worden.

Artikel 9

In het belang van de dienst kunnen de personeelsleden buiten de gewone arbeidsduur worden opgeroepen. Niemand mag zich aan deze oproep onttrekken, tenzij er een gegronde reden is. Voor deze prestaties zal compensatierust worden toegekend.

Artikel 10

Als normale rustdagen worden beschouwd : de zaterdagen, de zondagen, de wettelijke feestdagen, de dagen die een wettelijke feestdag vervangen, de facultatieve verlofdagen en het reglementair verlof.

Artikel 11

De normale rustpauzes zijn vervat in de uurregelingen, zoals opgenomen in bijlage 1.

Artikel 12 - Overuren

Opgeheven 05 oktober 2017

Artikel 13 – Niet toegelaten activiteiten

Zijn niet toegelaten tijdens de werkuren :

- consultaties en medische behandelingen;

- persoonlijke bezoeken, telefoongesprekken, fax en e-mail behalve in geval van dringende noodzakelijkheid en met voorafgaande toestemming van de secretaris.
- persoonlijk werk.

V. VERLOF

Art. 14 Algemeen

Opgeheven 05 oktober 2017

Art. 15 - Feestdagen

Opgeheven 05 oktober 2017

Art. 16 - Jaarlijkse vakantie

Opgeheven 05 oktober 2017

VI. BEZOLDIGING.

Artikel 17

Opgeheven 05 oktober 2017

Artikel 18

De uitbetaling van de lonen en wedden geschiedt volgens de wijze voorzien in de wet van 12 april 1965.

Artikel 19

Betalingen aan derden wordt slechts toegestaan op voorwaarde dat de aangeduide persoon drager is van een volmacht.

Artikel 20

Elk personeelslid ontvangt maandelijks een loonstrookje waarop de nodige inlichtingen staan in verband met de weddenberekening.

Eventuele betwistingen dienaangaande moeten zo spoedig mogelijk aan de secretaris worden voorgelegd.

Artikel 21

Bij beëindiging van de aanstelling of arbeidsovereenkomst is de laatste verschuldigde wedde ten vroegste opeisbaar op de normale betalingsdag.

VII. RECHTEN EN PLICHTEN VAN HET TOEZICHTHOUDEND PERSONEEL

Artikel 22

Het personeel belast met de leiding en het toezicht over het werk, vervangt de hogere leiding, elk volgens de hem/haar verleende bevoegdheid.

Het toezichthoudend personeel formuleert voorstellen en adviezen, voert onderzoeken uit, doet effectief toezicht op de correcte toepassing van instructies, arbeidsmiddelen, beschermings-middelen en procedures. Het toezichthoudend personeel wint hierover tijdig advies in bij de preventieadviseur.

In het bijzonder is het toezichthoudend personeel belast met :

- de controle op de aanwezigheid,
- de werkverdeling,
- de controle op het geleverde werk,
- de normale werking der machines; ingeval van breuk of ander defect moeten zij hun rechtstreekse chef verwittigen,
- het doen naleven van dienstnota's,
- het behoud van orde en tucht in de instellingen,
- het doen naleven van alle maatregelen die in het OCMW zijn getroffen of die zich opdringen voor het welzijn van het personeel.

Zij hebben het recht om vast te stellen dat een personeelslid die zich op het werk aanbiedt, klaarblijkelijk niet geschikt is om te werken en hem te verbieden het werk te beginnen, zonodig na ruggespraak met een geneesheer.

Wanneer een lid van het toezicht houdend personeel afwezig is, wordt hij vervangen. De plaatsvervanger(s) krijgt(en) dezelfde rechten en plichten.

De hiërarchische lijn heeft de plicht om gevallen van geweld, pesten of ongewenst seksueel gedrag te helpen voorkomen door deze tijdig te zien en niet te tolereren.

Het toezichthoudend personeel is er toe gehouden de regelen van rechtvaardigheid, onpartijdigheid, beleefdheid en welvoeglijkheid in acht te nemen.

VIII. BESCHERMING OP HET WERK

Artikel 23

De werknemers moeten zorg dragen voor hun eigen veiligheid en gezondheid en deze van de andere betrokken personen. Zij moeten op de juiste wijze gebruik maken van de hun ter beschikking gestelde arbeidsmiddelen en beschermingsmiddelen.

De werknemers moeten de gegeven instructies, vastgelegde werkwijzen en ingestelde procedures correct toepassen. Zij moeten ieder gevaar melden als het de veiligheid in het gedrang brengt en ook dadelijk de eerste maatregelen treffen.

Artikel 24

De bijzondere veiligheidsvoorschriften, die in het OCMW in acht moeten worden genomen, worden telkens als het nodig is, aan de personeelsleden bekend gemaakt.

Artikel 25

De personeelsleden kunnen hun maaltijden gebruiken in de ruimte die hiertoe door het OCMW wordt ingericht. Nochtans kan aan het personeel toelating verleend worden de maaltijd te gebruiken op de dienst.

Artikel 26

In uitvoering van de Wet op het Welzijn, haar uitvoeringsbesluiten en de toepassing van Titel II, Hoofdstuk III, afdeling I (Codex Welzijn) zijn bepaalde categorieën van personeelsleden onderworpen aan een wettelijk verplicht medisch onderzoek. Het medisch onderzoek van bedoelde personeelsleden is ook verplicht bij aanwerving, werkhervatting, werkpostverandering en bij zwangerschap/lactatie. Elk personeelslid kan ook zelf een medisch onderzoek aanvragen (spontane consultatie).

Niemand mag zich onttrekken aan het voorgeschreven medisch onderzoek en/of de verreiste medische technische prestatie.

Voornoemde verplichte medische onderzoeken en in voorkomen de vereiste medische technische prestaties gebeuren voor rekening van het OCMW.

Artikel 27

De personeelsleden die krachtens de wetgeving preventief moeten worden ingeënt, dienen zich op de hiervoor vastgestelde dag te melden.

Niemand mag zich aan deze verplichting onttrekken, tenzij mits voorlegging van een bewijs dat de inenting door een andere geneesheer werd verricht.

Het OCMW kan in het kader van de wetgeving of op advies van de arbeidsgeneesheer de lijst der preventieve inentingen uitbreiden, wanneer daartoe gegronde redenen bestaan.

Wanneer er gegronde redenen bestaan, kan in dringende gevallen op doktersadvies een bepaalde preventieve inenting opgelegd worden.

Artikel 28

De bijzondere hygiënevoorschriften die in de instellingen moeten worden in acht genomen, worden telkens als het nodig is aan de personeelsleden bekendgemaakt.

Artikel 29

Een verbandkast bevindt zich op de dienst bevolking van het stadhuis (tevens zetel van het OCMW).

Artikel 30 – Afwezigheid wegens arbeidsongeschiktheid tengevolge van ziekte of ongeval

In geval van arbeidsongeschiktheid wegens ziekte of ongeval dient het personeelslid volgende richtlijnen in acht te nemen :

§ 1. Verwittiging.

Behoudens overmacht, dienen de personeelsleden de secretaris van hun arbeids-ongeschiktheid te verwittigen op de eerste werkdag, hetzij telefonisch, hetzij op welke andere wijze dan ook.

Wanneer het personeelslid tijdens de arbeidsongeschiktheid eventueel niet thuis verblijft, dient hij/zij het adres van de verblijfplaats aan de secretaris mee te delen.

§ 2. Geneeskundig getuigschrift.

Als de ziekte een afwezigheid van meer dan 24 uur met zich meebrengt dan moet deze bevestigd worden door een geneeskundig getuigschrift overhandigd aan of verzonden aan de secretaris uiterlijk de tweede werkdag van de afwezigheid. De postdatum geldt als verzendingsdatum. Een afwezigheid van minder dan 24 uur wegens lichte ongesteldheid dient niet door een doktersattest bevestigd te worden maar is beperkt tot 1 dag per maand en vier dagen per kalenderjaar.

Het doktersgetuigschrift mag niet uitgaan van een geneesheer behorend tot het gezin van het personeelslid, noch van een bloed- of aanverwant in de 1ste of 2de graad.

In het attest laat het personeelslid de dokter de datum van het onderzoek vermelden, de aanvangsdatum van de arbeidsongeschiktheid, de vermoedelijke duur van de afwezigheid en de eventuele toelating om de woning te verlaten. De dag voor de vermoedelijke ziekteverlenging moet het zieke personeelslid contact opnemen met de secretaris. Wanneer het personeelslid geen contact opneemt met de secretaris, wordt het geacht het werk te hervatten op de volgende werkdag.

Indien de periode van ongeschiktheid langer duurt dan de voorziene datum, licht het personeelslid onmiddellijk, en ten laatste bij het aanvangsuur van de voorziene normale arbeidsprestatie de secretaris in over de verlenging en moet het personeelslid uiterlijk de tweede werkdag na het verlopen van de eerste arbeidsongeschiktheidsperiode een nieuw doktersattest inleveren of opsturen.

§ 3. Controleverplichting.

Het controletoezicht op de zieke personeelsleden zal uitgevoerd worden door een controlegeneesheer die door het OCMW wordt aangeduid.

Het personeelslid, afwezig ten gevolge van arbeidsongeschiktheid, dient zich aan deze controles te onderwerpen.

§ 4. Betwistingen.

Ingeval de controlerende geneesheer niet akkoord gaat met de beslissing van de behandelende geneesheer, neemt de controlegeneesheer eerst contact op met de behandelende geneesheer om tot een mogelijk vergelijk te komen.

Ingeval het niet tot een akkoord komt, zullen de controlerende geneesheer en de geneesheer van het personeelslid in onderling overleg een arts-scheidsrechter aanduiden.

§ 5. Arbitrageprocedure.

De aanwijzing van een arts-scheidsrechter moet gebeuren binnen de 2 werkdagen nadat de controlearts aan de werknemer zijn bevindingen overmaakte. De arts-scheidsrechter voert zijn onderzoek uit binnen de 3 werkdagen na zijn aanwijzing.

De uitspraak van deze arts is bindend voor beide partijen en zij zullen zich naar zijn oordeel schikken. De kosten van de scheidsrechterlijke procedure vallen ten laste van de verliezende partij.

Zolang er geen arts-scheidsrechterlijke beslissing is wordt het personeelslid als arbeidsongeschikt beschouwd.

De scheidsrechterlijke procedure doet geen afbreuk aan het recht der partijen om het geschil door de arbeidsrechtbank te laten beslechten.

§ 6. Verlof wegens verminderde prestaties wegens ziekte of ongeval.

Indien de arbeidsgeneesheer van oordeel is dat een wegens ziekte of ongeval in het privé-leven, afwezig personeelslid geschikt is om zijn/haar ambt terug op te nemen met halve dagprestaties, geeft het hiervan onmiddellijk kennis aan de OCMW-voorzitter.

De OCMW-voorzitter kan het personeelslid opnieuw in dienst roepen en de toelating verlenen te komen werken in een stelsel van verminderde prestaties als dit verenigbaar is met de goede werking van de dienst.

Een contractueel personeelslid dient eveneens de toelating te hebben van de medisch adviseur.

IX. BIJZONDERE VERPLICHTINGEN VAN HET PERSONEELSLID

Artikel 31

Met het oog op een juiste toepassing van de sociale en fiscale wetgeving zal het personeelslid bij de indiensttreding zijn naam, zijn adres, zijn verblijfplaats, zijn rijksregisternummer, zijn burgerlijke staat, zijn gezinstoestand en zijn nationaliteit meedelen. Het personeelslid zal bij wijziging van deze persoonlijke gegevens onmiddellijk de secretaris hiervan op de hoogte brengen.

Artikel 32

Elk personeelslid is in zijn beroepsbezigheid tot het beroepsgeheim en tot de grootste discretie gehouden.

Artikel 33

Het is niet toegelaten :

- een andere arbeid te verrichten dan deze welke werd opgelegd of tot de normale taak behoort;
- alcoholische dranken te gebruiken tijdens de werkuren of zich in dronken toestand op het werk te bevinden;
- te roken, tenzij in de daartoe bestemde lokalen;
- drukwerken of geschriften te verspreiden of uit te hangen, zonder voorafgaandelijke visering door de secretaris;
- politieke, filosofische of commerciële propaganda te verspreiden via meetings, folders of affiches;
- geldinzamelingen te doen of voorwerpen te koop aan te bieden, tenzij er voor dit alles een geschreven toelating is van het OCMW;
- geschenken of fooien te aanvaarden;
- zonder toestemming van de secretaris de dienst te verlaten onder de normale diensturen voor persoonlijke aangelegenheden.

Artikel 34

Het personeelslid is verplicht bij uitdiensttreding alle bezittingen (sleutel, badge, kledij, schoeisel, enz…) in te leveren bij het OCMW.

X. STRAFFEN

Artikel 35

Tekortkomingen op de verplichtingen door een statutair personeelslid kunnen aanleiding geven tot een tuchtprocedure.

Ten aanzien van contractuele personeelsleden die tekortkomen in hun verplichtingen, kunnen sanctionerende maatregelen genomen worden door de OCMW-raad, steeds rekening houdende met de belangen van het personeelslid op gebied van verdediging en voorafgaandelijk verhoor.

Het personeelslid behoudt het recht op de beoordelingsbevoegdheid van de rechtbanken en van de Raad van State.

XI. BESCHERMING VAN DE PERSONEELSLEDEN TEGEN GEWELD, PESTERIJEN EN ONGEWENST SEXUEEL GEDRAG OP HET WERK

Artikel 36 § 1. Begripsomschrijving.

Onder geweld wordt verstaan : “elke feitelijkheid waarbij een werknemer of een ander persoon psychisch of fysiek wordt lastiggevallen, bedreigd of aangevallen bij de uitvoering van het werk”.

Onder pesterijen wordt verstaan : “elke onrechtmatigheid en terugkerend gedrag, buiten of binnen het OCMW, dat zich inzonderheid kan uiten in gedragingen, woorden, bedreigingen, handelingen, gebaren en eenzijdige geschriften en dat tot doel of gevolg heeft dat de persoonlijkheid, de waardigheid of de fysieke of psychische integriteit van een werknemer wordt aangetast, dat zijn betrekking in gevaar wordt gebracht of dat een bedreigende, vijandige, beledigende, vernederende of kwetsende omgeving wordt gecreëerd.”

Onder ongewenst seksueel gedrag op het werk wordt verstaan : “elke vorm van verbaal, niet-verbaal of lichamelijk gedrag van seksuele aard waarvan degene die zich er schuldig aan maakt, weet of zou moeten weten dat het afbreuk doet aan de waardigheid van vrouwen en mannen op het werk.”

§ 2. Beginselverklaring.

Elke werknemer – man of vrouw – heeft het recht met waardigheid behandeld te worden.

Elke werknemer heeft de plicht op positieve wijze bij te dragen tot het preventiebeleid dat wordt tot stand gebracht in het kader van de bescherming van de werknemers tegen geweld, pesterijen en ongewenst seksueel gedrag op het werk en erop te letten dat hij zijn collega’s op het werk met eerbied en waardigheid behandelt.

Elke werknemer heeft de verplichting zich te onthouden van gedrag dat aanleiding kan geven tot geweld, pesten of ongewenst seksueel gedrag op het werk (zowel verbaal als niet verbaal) en bij te dragen tot een arbeidsomgeving waarin de waardigheid van de medewerkers wordt geëerbiedigd.

Personeelsleden waarvan vastgesteld wordt dat zij zich bezondigen aan geweld, pesten of ongewenst seksueel gedrag op het werk begaan een zware fout, welke aanleiding kan geven

tot ontslag.

§3. De werkgever verbindt zich er toe dat alle nodige preventieve maatregelen zullen worden genomen om de werknemers te beschermen tegen geweld, pesterijen en ongewenst seksueel gedrag bij de uitvoering van het werk. Het betreft onder meer :

1. de materiële inrichting van de arbeidsplaatsen :
   - gescheiden toiletten en kleedkamers voor mannen en vrouwen;
   - voldoende bureau-oppervlakte per persoon;
   - voldoende verlichting en verluchting in de werkruimtes, gangen en lokalen;
   - het weren van provocerende affiches, posters, tijdschriften, …
   - het toekennen aan iedereen van de nodige uitrusting en communicatiemiddelen om zijn job naar behoren te kunnen uitvoeren;
2. de mogelijkheid om tijdens de werkuren (telefonisch) contact op te nemen met de vertrouwens-persoon;
3. het onthaal, de hulp aan en de ondersteuning van de slachtoffers;
4. voorzien in een vorm van periodieke communicatie rond de problematiek (dienstnota's, werkoverleg, vorming, …)

§ 4. Procedure.

Werknemers die menen het slachtoffer te zijn van geweld, pesten of ongewenst seksueel gedrag op het werk kunnen voor opvang en onmiddellijke hulp eerst terecht bij de hiervoor aangestelde vertrouwenspersoon of (nadien) bij de preventieadviseur.

De vertrouwenspersoon hoort het slachtoffer en de beschuldigde persoon afzonderlijk en poogt het probleem op informele wijze op korte termijn op te lossen. Wanneer de informele poging mislukt, kan het personeelslid, dat zich het slachtoffer voelt van geweld, pesten of ongewenst seksueel gedrag, zich wenden tot de preventieadviseur. Het betrokken personeelslid kan zich ook rechtstreeks wenden tot de preventieadviseur.

§ 4.1 Informele procedure.

a) In geval een vertrouwenspersoon wordt benaderd.

   De vertrouwenspersoon hoort het slachtoffer en bemiddelt op verzoek van het slachtoffer met de dader. Dit houdt in dat de vertrouwenspersoon aan de persoon die zich inlaat met geweld, pesterijen of ongewenst seksueel gedrag op het werk, duidelijk uitlegt dat zijn/haar gedrag ongepast is, of dat hij iemand in verlegenheid brengt en het werk stoort. Indien het ten laste gelegde gedrag blijft voortduren of indien de vertrouwenspersoon het niet aangewezen acht het probleem op informeel wijze op te lossen, raadt de vertrouwens-persoon de werknemer aan de formele procedure, met indiening van een met reden omklede klacht, te volgen.

b) In geval de preventieadviseur wordt benaderd.

   De bevoegde preventieadviseur hoort het slachtoffer en bemiddelt op verzoek van het slachtoffer met de dader. Dit houdt in dat de preventieadviseur aan de persoon die zich inlaat met geweld, pesterijen of ongewenst seksueel gedrag op het werk, duidelijk uitlegt dat zijn gedrag ongepast is, of dat hij iemand in verlegenheid brengt en het werk stoort. Indien het ten laste gelegde gedrag blijft voortduren of indien de preventieadviseur het niet aangewezen acht het probleem op informele wijze op te lossen, raadt de

preventieadviseur de werknemer aan de formele procedure, met indiening van een met redenen omklede klacht, te volgen.

§ 4.2 Formele procedure met indiening van een klacht.

Indien het probleem niet op informele wijze kan opgelost worden of indien het slachtoffer dit niet wenselijk acht, kan het slachtoffer een met reden omklede klacht indienen bij de vertrouwenspersoon of de bevoegde preventieadviseur.

De vertrouwenspersoon neemt de met redenen omklede klacht in ontvangst en zendt ze onmiddellijk door aan de bevoegde preventieadviseur.

De bevoegde preventieadviseur neemt de met redenen omklede klacht op in een geschreven, gedateerd en ondertekend document dat wordt aangevuld met de verklaringen van het slachtoffer en de eventuele getuigen en in voorkomend geval het resultaat van de bemiddeling. Het slachtoffer en de getuige(n) ontvangen een afschrift van hun verklaring. De bevoegde preventieadviseur geeft onmiddellijk een afschrift van het document aan het OCMW. In het kader van de behandeling van een klacht, zal het OCMW zich onthouden van maatregelen die neerkomen op de beëindiging van de arbeidsovereenkomst of eenzijdige wijziging van de arbeidsvoorwaarden ten opzichte van de werknemer die de klacht ingediend heeft of die een getuigenis heeft afgelegd in het raam van een klacht.

De preventieadviseur kan eventueel bijkomende onderzoeksdaden stellen. Het OCMW waarborgt dat zowel de vertrouwenspersoon als de preventieadviseur hun opdracht in alle onafhankelijkheid en autonoom kunnen uitvoeren en dat zij hiervoor de nodige tijd en ruimte krijgen. Dit onderzoek moet onafhankelijk en objectief zijn en moet onder volstrekte geheimhouding plaatsvinden (verslagen, gesprekken, notities, …).

Tijdens het onderzoek zal (zullen) de beklaagde perso(o)n(en) op de hoogte gebracht worden van alle details inzake de aard van de klacht en heeft/hebben hij/zij de mogelijkheid hierop zowel mondeling als schriftelijk te antwoorden. Hun mondeling antwoord zal echter bevestigd moeten worden met een geschreven stuk dat gedateerd en ondertekend werd.

Zowel het slachtoffer als de perso(o)n(en) die aangeklaagd wordt/worden, kunnen zich naar eigen keuze laten vergezellen en/of vertegenwoordigen door een collega op het werk, een externe raadgever, een vertegenwoordiger van het personeel of een vakbondsafgevaardigde. Deze personen zijn ook verplicht tot geheimhouding.

De bevoegde preventieadviseur stelt een individueel klachtendossier samen en houdt het bij met daarin een volledig verslag van alle bijeenkomsten, tussenkomsten en onderzoeken, alle documenten en verklaringen en de vooropgestelde maatregelen evenals zijn persoonlijke aantekeningen en bevindingen. Enkel de bevoegde preventieadviseur en de vertrouwensperso(o)n(en) en de raadsman hebben toegang tot dit dossier. Zij mogen de gegevens waarvan zij kennis hebben niet bekend maken.

De preventieadviseur stelt een eindrapport op waarin, naargelang het geval, het bestaan van geweld, pesterijen en ongewenst seksueel gedrag op het werk vastgelegd of weerlegd wordt.

Dit rapport zal na het onderzoek en na voorafgaande inzage door het slachtoffer en de perso(o)n(en) die aangeklaagd wordt/worden aan het OCMW overhandigd worden en zal een voorstel bevatten met passende maatregelen.

Het OCMW neemt, wanneer het op de hoogte gebracht wordt van feiten van geweld, pesterijen of ongewenst seksueel gedrag op het werk, passende maatregelen om hieraan een einde te

maken. Indien ook de preventieadviseur niet tot een oplossing komt of wanneer het pestgedrag niet stopt, is hij/zij verplicht de medische inspectie in te schakelen. Deze inspectiedienst kan opnieuw een verzoeningspoging opstarten ofwel onmiddellijk een proces-verbaal starten.

§ 4.3 Procedure voor feiten extern aan het OCMW.

Werknemers die menen het slachtoffer te zijn van feiten van geweld, pesterijen of ongewenst seksueel gedrag op het werk, die extern zijn aan het OCMW, zijn ertoe gehouden hierover een verklaring af te leggen bij het OCMW (door de gemandateerde perso(o)n(en), de vertrouwenspersoon of de bevoegde preventieadviseur). Deze verklaring wordt opgenomen in een register over feiten van geweld op het werk. Alleen het OCMW, de preventieadviseur en de vertrouwenspersoon en de raadsman hebben toegang tot dit register.

§ 5 Wetgeving.

De inhoudelijke uitwerking van de wet zit vervat in een nota betreffende de nieuwe wetgeving “de bescherming tegen geweld, pesterijen en ongewenst seksueel gedrag op het werk” (cfr. Bijlage 2).

BIJLAGE 1 : UURREGELING VOOR DE DIVERSE DIENSTEN.

Maandag van 08.20 tot 12.00 uur en van 13.30 uur tot 17.30 uur
Dinsdag van 08.20 tot 12.00 uur en van 13.30 uur tot 17.30 uur
Woensdag van 08.20 tot 12.00 uur en van 13.30 uur tot 17.30 uur
Donderdag van 08.20 tot 12.00 uur en van 13.30 uur tot 17.30 uur
Vrijdag van 08.20 tot 12.00 uur en van 13.30 uur tot 17.30 uur

BIJLAGE 2 : Nota betreffende de nieuwe wetgeving aangaande “de bescherming tegen geweld, pesterijen en ongewenst seksueel gedrag op het werk”.

BIJLAGE 3 : Verlofreglement.

BIJLAGE 4 : Externe Dienst voor Preventie en Bescherming op het Werk

PROVIKMO
Maarschalk Fochlaan 34
8900 IEPER
Tel. 057 22 86 67

BIJLAGE 5 : Intergemeentelijke veiligheidsdienst.

BIJLAGE 6 : Controle-organisme in geval van ziekte.

MEDEX
Victor Hortaplein 40 bus 10
1060 BRUSSEL
Tel. 02 524 97 97

BIJLAGE 7 : Diensten voor sociale inspectie.

Ministerie van Tewerkstelling en Arbeid
Inspectie van de sociale wetten
Kleine Bassinstraat 16
8800 ROESELARE
tel. 051 20 29 16
fax 051 24 66 16

(ofwel Breidelstraat 3 te 8000 Brugge, tel. 050 44 20 30)

Ministerie van Tewerkstelling en Arbeid
Medische Inspectie
Administratief Centrum Ter Plaeten
Sint Lievenslaan 33 b
9000 GENT
tel. 09 235 29 82
fax 09 235 28 74

Ministerie van Tewerkstelling en Arbeid
Technische Inspectie
Breidelstraat 3
8000 BRUGGE
tel. 050 44 20 20
fax 050 44 20 29

Ministerie van Sociale Zaken, Volksgezondheid en Leefmilieu
Sociale Inspectie
Oude Gentweg 75c
8000 BRUGGE
tel. 050 44 59 70

BIJLAGE 8 : Samenstelling onderhandelingscomité.

Namens de overheid :	EVRARD Sandy, Voorzitter	
	NN	
	FLORISSOONE Patrick, algemeen directeur.	
Namens de vakbonden :	ACOD :	NN
	CCOD :	NN
	Liberale Vakbond :	NN

BIJLAGE 9: e-policy informatieverwerking

Inleiding

Waarom deze nota?

Deze policy is van toepassing op het gebruik van informatieverwerking in de breedste zin.
De policy regelt onder meer een efficiënt gebruik van de IT-middelen rekening houdend met alle nodige veiligheidsvoorzieningen ter bescherming van de IT-systemen, de informatieveiligheid en de belangen van de werkgever.
Gelet op de snelle technologische evoluties en de uitdagingen op vlak van dienstverlening, efficiëntie, informatie- en IT-veiligheid is het noodzakelijk om bij dringende situaties onmiddellijk te kunnen optreden in het belang van de werkgever. Bijgevolg kunnen er op ieder ogenblik extra maatregelen genomen worden buiten de bepalingen van deze policy. Deze worden dan ook via andere gebruikelijke meldingskanalen aan de personeelsleden meegedeeld.
Naleving van deze policy is een voorwaarde om toegang te verkrijgen en te behouden tot de IT-middelen.

Voor wie is deze nota bestemd?

De afspraken gelden voor iedereen die gebruikt maakt van IT-middelen die de werkgever ter beschikking stelt. Dit zijn in eerste instantie de werknemers, maar kan ook gelden voor medewerkers van andere organisaties die gebruik maken van diensten en IT-middelen die door de werkgever ter beschikking worden gesteld.
Het is mogelijk dat er binnen de verschillende intergemeentelijke samenwerkingsverbanden specifieke afspraken worden gemaakt. Indien (intergemeentelijke) medewerkers op het netwerk van Mesen werken,, dan moeten zij minimaal deze richtlijnen volgen.

Wat zijn IT middelen?

- IT middelen omvatten de **IT systemen** (hard- en software) die worden ingezet bij het uitvoeren van de taken en opdrachten. Voorbeelden hiervan zijn o.m.
- Internet- en e-mailfaciliteiten
- Computers, laptops, tablets, telefoons
- Printers
- USB-sticks en andere gegevensdragers
- Toepassingen en opslagsystemen
- …

Hoe omgaan met IT-middelen

Er wordt verwacht dat de gebruiker met de IT middelen omgaat als een goede huisvader. Dit houdt in dat men zich vooruitziend en zorgvuldig gedraagt. Men anticipeert en probeert de negatieve gevolgen van hun handelen redelijk in te schatten en problemen te voorkomen door het nemen van gepaste voorzorgsmaatregelen.
Daarnaast beseft de gebruiker dat de middelen dienen om het belang van de werkgever en de doelen van de organisatie te ondersteunen.
het Lokaal Bestuur Mesen doet een beroep op Pieters IT (hierna genaamd de IT-dienst) voor IT ondersteuning. Bij IT-problemen neemt de gebruiker onmiddellijk contact op met de dienst IT en dit volgens de geldende richtlijnen.

Beroepsmatig gebruik is de norm

De door de werkgever ter beschikking gestelde IT-middelen mogen in principe enkel voor **professionele doeleinden** gebruikt worden.
De werkgever staat echter een uitzonderlijk én beperkt gebruik van internet, e-mail en sociale media voor privédoeleinden toe onder volgende voorwaarden:

Privégebruik:

- Mag het werk, de prestaties, de dienstverlening niet beïnvloeden;
- Is occasioneel en beperkt in tijd;
- Mag niet storend zijn voor collega's en dienst;
- Mag de goede werking en veiligheid van de IT-middelen niet in het gedrang brengen;
- Mag de belangen en veiligheid van de werkgever niet schaden.

Ook bij dergelijk strikt beperkt en sporadisch gebruik van internet, e-mail en sociale media voor privédoeleinden blijft de gebruiker gebonden door de bepalingen van deze policy.
In de mate dat privégebruik toegestaan is, gaat het om een gunst en niet om een recht, dat steeds kan ingeperkt of ingetrokken worden. Het opslaan van privégegevens (bv. muziek, documenten, etc.) op de IT-middelen van de werkgever is verboden.
Het is verboden om andere e-mailsystemen (Gmail, Hotmail, Yahoo, …) te gebruiken dan deze die door de werkgever ter beschikking worden gesteld of toegestaan zijn.

E-mail

Algemeen

- E-mails die worden verstuurd vanuit het professionele adres (voornaam.naam@mesen.be) of vanuit generieke e-mailadressen worden verondersteld om werk-gerelateerd te zijn.
- Generieke e-mailadressen kunnen door verschillende personen (meestal binnen dezelfde dienst) gebruikt worden. Dergelijke mailboxen worden uitsluitend als werk-gerelateerd en niet-privé beschouwd.
- Privémail kan wel gebruikt worden via het publieke WIFI-netwerk (bijv. via de smartphone).

Richtlijnen

Bij gebruik van e-mail dienen een aantal regels gevolgd te worden:

- Wees alert. E-mail wordt misbruikt voor spam, voor het verspreiden van virussen en schadelijke software (malware) en om vertrouwelijke informatie te weten te komen. Mogelijke indicaties van verdachte e-mail zijn:
  - ongekende afzender
  - onverwachte of ongekende context (onderwerp, inhoud, taal)
  - bijlagen
  - hyperlinks

Bij de minste twijfel mag de gebruiker geen bijlagen of hyperlinks openen. Vraag raad bij de externe IT'er.

- Gebruik e-mail niet voor het versturen van persoonsgevoelige gegevens.

Het is **verboden**:

- deel te nemen aan kettingbrieven, spamming en dergelijke.
- e-mailberichten te versturen in de hoedanigheid van een ander persoon.
- interne bedrijfsinformatie door te sturen naar derden die niet professioneel bij het proces betrokken zijn of waarvoor deze info niet is bestemd.
- vertrouwelijke e-mail door te sturen naar een externe mailbox.

Deze lijst dient als voorbeeld en is niet limitatief.

Bij afwezigheid

Conform de bovenvermelde richtlijnen worden wachtwoorden tijdens afwezigheden niet gedeeld.
Personeelsleden die langer dan 1 dag afwezig zijn, stellen zelf een afwezigheidsbericht in hun mailbox in.
Als automatisch antwoord kan dan bijvoorbeeld volgende tekst worden gebruikt:
"Ik ben afwezig/met verlof van (datum) t.e.m. (datum). Tijdens mijn afwezigheid worden mijn e-mails niet gelezen. Voor dringende zaken kan u contact opnemen met mijn collega('s) via naam.voornaam@mesen.be of dienst@mesen.be".
Ingeval van hoogdringendheid én noodzakelijkheid kan de algemeen directeur toegang verlenen aan de IT-dienst.
Dit onder volgende voorwaarden:

- De opzoeking is hoogdringend: de leidinggevende dient te motiveren waarom er niet op de terugkeer van het personeelslid gewacht kan worden.
- De opzoeking is noodzakelijk: de informatie is nodig in kader van de continuïteit van de werking van de dienst.

- Ingeval van een positieve beslissing wordt het personeelslid gecontacteerd met de vraag tot expliciete toestemming inzake toegang tot de mailbox (bijv. bij langdurige afwezigheid).
- Het personeelslid verleent géén expliciete toestemming (bijv. bij ongeval, onvoorziene omstandigheden, manifest misbruik van de account enz.: in dit geval beslist de algemeen directeur of de toegang door noodzakelijk is.
- Het personeelslid (IT-dienst) die toegang krijgt tot een persoonlijke mailbox van een collega, beperkt zich uitsluitend tot de professionele e-mails en enkel voor het specifieke doel van de opzoeking.

Bij uitdiensttreding

Wanneer een personeelslid de organisatie verlaat, zorgt hij zelf ervoor dat alle werkgerelateerde informatie gearchiveerd is en ontsloten kan worden naar anderen. De leidinggevende ziet hierop toe.

Wanneer een personeelslid het bestuur verlaat, krijgt het personeelslid de gelegenheid om alle persoonlijke e-mails (privé-communicatie met arbeidsgeneesheer, IDEWE, vertrouwenspersoon, etc.) te verwijderen of door te sturen naar een persoonlijk mailadres. Alle overige e-mails in mailbox worden geacht professioneel te zijn.

Na uitdiensttreding wordt de toegang tot de mailbox geblokkeerd en wordt er een automatisch antwoord ingesteld:

“Ik ben niet langer werkzaam in het Lokaal Bestuur Mesen. Deze mailbox wordt binnenkort gedeactiveerd en inkomende e-mails worden niet gelezen. Gelieve uw e-mail opnieuw te versturen naar naam.voornaam@mesen.be of dienst@mesen.be”.

Na een periode van 1 maand (3 maanden bij leidinggevende functies) wordt de mailbox gedeactiveerd.

Omwille van de continuïteit van de dienstverlening en de goede werking, mag de werkgever de mailbox – na het deactiveren – exporteren in een PST-file. Deze file wordt tijdelijk gearchiveerd in een beveiligde omgeving (minstens 1 jaar, 2 jaar voor een directeursfunctie).

Enkel op uitdrukkelijk verzoek van de algemeen directeur kunnen er nog e-mails geraadpleegd worden (vb. communicatie met een dossierbehandelaar van het Agentschap Binnenlands Bestuur).

Enkel de IT-dienst kan opzoekingen doen. Dergelijke raadplegingen zijn zeer uitzonderlijk en enkel bij noodzakelijkheid.

Bij een gedwongen vertrek, wordt de toegang tot mailbox meteen geblokkeerd en stelt de IT-dienst een automatisch antwoord in.

Het personeelslid krijgt binnen de 10 werkdagen na het ontslag de gelegenheid om de mailbox op te schonen. Bij een geschil kan de algemeen directeur vragen dat dit wordt uitgevoerd in het bijzijn van een derde neutrale partij/ vertrouwenspersoon (externe preventieadviseur, etc.).

Bovenstaande richtlijnen inzake bewaring en raadpleging blijven van toepassing.

Internet

De werkgever voorziet zijn gebruiker van een toegang tot het internet voor professionele doeleinden.

Het is echter **verboden**:

- de internettoegang van de werkgever te gebruiken om in te breken in netwerken (hacken).
- vertrouwelijke informatie via internet te verspreiden
- te surfen naar pornografische, discriminerende of racistische websites.
- netwerken voor anonieme communicatie (bijv. Tor-browser) en peer-to-peer netwerken voor gegevensuitwisseling (bijv. BitTorrent) te gebruiken.
- op internet te spelen, te gokken, etc.
- software, muziek of video te downloaden en te uploaden indien dit in strijd is met de wet op de auteursrechten.

Deze lijst dient als voorbeeld en is niet limitatief.

De werkgever behoudt zich het recht voor om op elk moment de toegang tot websites, waarvan hij de inhoud ongepast vindt, te blokkeren. De werkgever heeft het recht om de internetconnectie volledig of gedeeltelijk uit te schakelen of de connectie in tijd te beperken.
Hou ermee rekening dat de meeste websites bij raadpleging een spoor nalaten. In bepaalde gevallen identificeren websites heel precies de herkomst van de bezoeker alsook zijn elektronische identificatie (in deze omstandigheden die van de werkgever).

Wachtwoorden

Algemeen

Het gebruik van het wachtwoord en het account zijn **strikt persoonlijk** en **vertrouwelijk**. Elke gebruiker is persoonlijk verantwoordelijk voor de zorgvuldige en vertrouwelijke omgang met de eigen wachtwoorden en voor alles wat onder zijn/haar account gebeurt.
Het is verboden om de persoonlijke account door anderen te laten gebruiken. Het is verboden wachtwoorden aan anderen mee te delen of op enige andere wijze onveilig te bewaren. Wachtwoorden mogen niet op een zichtbare wijze of op een voor derden toegankelijk medium bewaard worden.

Richtlijnen

- Hoe langer een wachtwoord hoe beter. Het wachtwoord moet minstens 10 karakters hebben.
- Mix hoofdletters, kleine letters en tekens door elkaar: gebruik minimaal drie van de vier categorieën uit volgende tekens in het wachtwoord:
  - Hoofdletters
  - Kleine letters
  - Cijfers
  - Niet-alfanumerieke karakters
- Hulpmiddelen voor een goed wachtwoord kunnen zijn:
  - Werk met een wachtwoordzin. Bijv. Ik ga iedere dag naar het bos!
  - Stop er iets in wat je zelf makkelijk kunt onthouden, maar door iemand anders heel moeilijk te achterhalen valt.
  - Zorg dat je een paswoord hebt wat je heel snel kunt intypen. Dit verkleint de kans dat iemand anders het paswoordje te weten komt.
- Beter niet gebruiken:
  - Naam, voornaam, geboortedatum, ….
  - Voor de hand liggende woorden, herhalingen van getallen, nummerreeksen, etc.
- Schrijf paswoorden best niet op. Als je dit toch doet, hou het wachtwoord dan zeker niet bij in de buurt van de PC of laat het niet op het bureel rondslingeren.
- Indien je een twee-factor authenticatie kunt gebruiken, is het absoluut aan te raden om dit te gebruiken.
- Wachtwoorden moeten regelmatig worden gewijzigd. Jaarlijks zal het systeem op 01 juni een automatische melding geven om je wachtwoord (Windows login) aan te passen. Een gebruiker kan dit ook steeds op eigen initiatief.

Downloaden van software

Installeren van software op PC's en laptops wordt in principe niet verhinderd (vb. toevoegen nieuwe printers, etc.). Indien – om wille van de taak of het werk – toch specifieke software gedownload moet worden vanop het internet, wordt de dienst IT het best gecontacteerd zodat zij kunnen kijken of er eventuele alternatieven zijn. Indien er tijdens het downloaden een melding komt van de antivirus moet de gebruiken meteen de IT-dienst verwittigen.

Gebruik van opslagsystemen

- Opslag van documenten is alleen toegelaten op IT-middelen die door de werkgever ter beschikking gesteld worden.
- Documenten worden bewaard op de netwerkschijf of in specifieke toepassingen, waarvan dagelijks een reservekopie (back-up) gemaakt wordt. Hierdoor is het overbodig dat gebruikers zelf back-ups nemen.
- Van documenten die bewaard worden op de harde schijf van de computer wordt geen reservekopie genomen. Bovendien is er een reëel risico dat deze documenten

verloren gaan bij een technisch defect (crash), bij verlies of diefstal of bij vervanging van de computer. Hetzelfde geldt voor documenten bewaard op een tablet of smartphone. Bewaring zoals hier vermeld is volledig op eigen verantwoordelijkheid.

- Opslag van documenten is verboden op dragers die niet ter beschikking gesteld worden door de werkgever. Hieronder vallen onder andere:
  - eigen USB-stick, externe harde schijf, laptop, tablet, smartphone enz.
  - zogenaamde cloud opslag die niet in het beheer van de werkgever zijn (zoals bv. Google Drive, Dropbox,). Toegelaten toepassingen zoals de OneDrive of SharePoint van het bestuur zijn toegelaten.

Ecologische voetafdruk

Ook bij het gebruik van IT middelen zijn een aantal maatregelen te nemen om bewust om te springen met energie en de druk op het milieu niet onnodig te verhogen.

- Zet je PC en scherm uit indien je naar huis vertrekt.
- Voor kortere onderbrekingen kun je gebruik van de slaap- of stand-by stand.
- Zet projectoren en schermen uit na het gebruik van vergaderzalen.

Clear desk – clean screen

- Laat geen gevoelige data op je bureau of op de printer liggen, berg deze op het einde van de werkdag op in een map of kast en sluit je bureau af (indien mogelijk). Vernietig papieren met gevoelige gegevens in de papierversnipperaar of laat ze vernietigen door een gespecialiseerde firma.
- Vergrendel je PC of meld je af bij het verlaten van je werkplek.

Gebruik eigen mobiele toestellen

De gebruiker gebruikt bij de uitvoering van zijn taken alleen IT-middelen die door de werkgever ter beschikking gesteld worden.

Bij mobiele toestellen die professionele IT-systemen benaderen (bv. mail of agenda synchroniseren, toegang tot bestanden, etc.) is het verplicht om minstens een patroon, pincode of vingerafdruk te gebruiken om het toestel te kunnen ontgrendelen.

Het is toegelaten om de eigen smartphone en tablet te gebruiken met de daarvoor voorziene Wifi-netwerken en internetverbinding. Het e-mailaccount mag gekoppeld worden aan deze toestellen. De gebruiker voorziet een gepaste beveiliging van zijn toestel. Via zijn Office 365 account kan de gebruiker via de Office 365 Mobile Device Manager zijn toestel beheren en bij verlies op afstand wissen.

Telewerken

Telewerk is noch een recht, noch een plicht, maar een afspraak tussen de leidinggevende en het personeelslid. Het personeelslid moet vooraf toestemming hebben van de algemeen directeur voor het telewerk. In een overmacht situatie kan bij aanvang nog toestemming gevraagd worden.

Structureel telewerk, bijvoorbeeld een vaste thuiswerkdag, wordt niet toegestaan.

Transport

Voor het transporteren van toestellen (laptops, projectors, etc.) wordt verondersteld dat de gebruiker de nodige voorzorgen neemt om dit op een veilige manier te zien zodat de toestellen niet beschadigd raken.

Verlies

Indien de gebruiker zijn laptop, tablet of telefoon verliest, moet dit onmiddellijk worden gemeld bij de algemeen directeur én DPO.

Indien de gebruiker zijn tablet of telefoon verliest en zijn werkmail en –agenda synchroniseert met een mobiel toestel, dient deze het toestel onmiddellijk te wissen.

Nieuwsbrieven

- Het versturen van nieuwsbrieven is één van de manieren om burgers te informeren over de werking van het lokaal bestuur. Vraag steeds expliciet toestemming vooraleer je een nieuwsbrief verstuurt. Het is de burger die bepaalt welke nieuwsbrieven hij of zij ontvangt.

- Zorg dat er steeds een uitschrijflink in de nieuwsbrief is opgenomen. Respecteer de wens van de burger om niet langer aangeschreven te worden en verwijder de contactgegevens uit het adressenbestand.

Beeldmateriaal

- Vraag steeds toestemming bij het nemen en gebruiken van gerichte beelden (close-up, focus op de personen op de foto).
- Informeer deelnemers van activiteiten bij de inschrijving dat er sfeerfoto's zullen genomen worden.

Meer informatie en voorbeelden uit de praktijk is terug te vinden in de handleiding "Recht op afbeelding". Dit document is raadpleegbaar in de publieke map op de server of kan opgevraagd worden bij de DPO.

gedragscode

Omgaan met sociale media

Met de komst van sociale media verandert de manier van werken, communiceren en kennis delen. De interactie tussen veel verschillende mensen biedt veel kansen, maar kan ook minder gewenste gevolgen hebben. Daarom is het belangrijk spelregels te bepalen die iedereen kent en volgt. Deze spelregels zijn zowel bedoeld voor de gebruikers die sociale media werk-gerelateerd inzetten, maar evengoed voor privégebruik.

De gebruiker wordt gevraagd om volgende 2 basisprincipes te respecteren als hij sociale media gebruikt met een (on)rechtstreekse link naar de werkgever.

<u>Sociale media zijn zichtbaar</u>

- De gebruiker dient zich ervan bewust te zijn dat alles wat hij meedeelt op sociale media (lange tijd) vindbaar is en ook tegen zichzelf of de werkgever gebruikt kan worden. Daarom volgende richtlijnen:
- Deel geen vertrouwelijke informatie mee op sociale media.
- Plaats niet zomaar afbeeldingen van personen op sociale media zonder hun toestemming.
- Spreek je als gebruiker niet kritisch uit over collega's, burgers en familie, leveranciers, overheden en de werkgever.
- Problemen op de werkvloer worden niet besproken op sociale media
- De gebruiker is persoonlijk verantwoordelijk voor de inhoud die hij publiceert op de sociale media.

<u>Sociale media zijn een vorm van (positieve) communicatie</u>

- Sociale omgangsvormen gelden ook online. Alles wat je schrijft, formuleer je op een respectvolle, positieve en professionele manier.
- Laster, beledigingen en obsceniteit zijn verboden.
- Spreek steeds in eigen naam en niet in naam van de werkgever. Alles wat je plaatst en het imago van de werkgever schaadt, is uiteindelijk je eigen verantwoordelijkheid.
- De werkgever kan negatief in het nieuws komen door ongepaste berichten op sociale media van eigen personeelsleden en berichten op sociale media kunnen leiden tot controverse. Houd er daarnaast wel rekening mee dat, ondanks het feit dat je niet namens de werkgever spreekt, je wel steeds geassocieerd wordt met de werkgever.
- De werkgever hecht veel belang aan een warme omgang in de relatie gebruiker-burger, maar verwacht een goede balans tussen afstand en nabijheid en dit zowel met de burger als zijn naaste omgeving. Het is de verantwoordelijkheid van de gebruiker om deze balans in evenwicht te houden en er zich bewust van te zijn dat toegang tot het privéleven van de gebruiker in de vorm van sociale media, verwarrend en belastend kan werken voor een gezonde balans.

<u>Gebruik sociale media tijdens het werk</u>

Gebruikers mogen tijdens het werk actief zijn op sociale media als ze gebruikt worden voor professionele doeleinden. Ook in sociale media ben je gebonden door je beroepsgeheim. Bij twijfel of een bepaalde publicatie in strijd is met deze policy of indien de online communicatie dreigt te ontsporen, neemt de gebruiker contact op met zijn/haar leidinggevende.

Gebruik van telefoon
De telefoontoestel dat de werkgever aan de gebruiker ter beschikking stelt, wordt in principe alleen voor professioneel gebruik aangewend.
De werkgever tolereert evenwel het exceptioneel gebruik van telefoon en fax voor privédoeleinden, op voorwaarde dat dit gebruik occasioneel is en in niets de goede gang van zaken binnen de dienst beïnvloedt.
De werkgever heeft het recht om naargelang de functie of dienst een preventieve beperking in te stellen op de extern te bereiken nummers (bijv. inzake betaalnummers of buitenlandse nummers).
Gebruik van briefwisseling en briefgeheim
De werkgever kan er van uitgaan dat de briefwisseling die op adres van de werkgever toekomt te beschouwen is als professionele briefwisseling waarvan hij in principe kennis kan nemen. Hij kan deze brieven openen en behandelen.
Een brief met vermelding van het adres van de werkgever en met vermelding van de naam van een gebruiker en met de duidelijke vermelding 'persoonlijk en vertrouwelijk' (of gelijkaardig) wordt beschouwd als privébriefwisseling en is beschermd door het briefgeheim.
Contacten met de media (krant, radio, etc.)
Het imago van de werkgever wordt in belangrijke mate bepaald door verslaggeving in de media. Daartoe is de door de werkgever verstrekte informatie van cruciaal belang.
Contacten met de media in naam van de werkgever behoren dan ook enkel tot de bevoegdheid van de personeelsleden die door de werkgever aangewezen zijn als woordvoerder:

- De algemeen directeur
- Ad hoc aangewezen personen

De overige personeelsleden dienen zich te onthouden van publieke verklaringen met betrekking tot de werkgever, die de werkgever (kunnen) verbinden of in diskrediet (kunnen) brengen.
Tevens verwijzen we hierbij naar de bepalingen betreffende het beroepsgeheim en behandelen van vertrouwelijke informatie en de afsprakennota communicatie.

Informatieveiligheid en GDPR

Informatieveiligheid
Onder informatieveiligheid verstaan we het geheel van maatregelen, procedures en processen die de beschikbaarheid, integriteit en vertrouwelijkheid van alle vormen van informatie garanderen.
Beschikbaarheid is het waarborgen dat geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot de informatie en informatiesystemen.
Integriteit staat in het teken van het behouden en beschermen van de juistheid en de consistentie van data en het voorkomen dat data onbedoeld aangepast worden.
Vertrouwelijkheid is het waarborgen dat informatie alleen toegankelijk is voor diegenen die hiertoe zijn geautoriseerd.
Het **informatieveiligheidsplan** dient als leidraad voor de aansturing en coördinatie van de verschillende beveiligingsprocessen. Het uiteindelijke doel is het inrichten van een evenwichtig stelsel van beveiligingsmaatregelen, gericht op risicobeheersing.
Verwerking van persoonsgegevens

- Lokale overheden beschikken over heel wat **persoonsgegevens**, dit zijn gegevens waarmee je een natuurlijk persoon kunt identificeren (naam, adres, rijksregisternummer, rekeningnummer, e-mailadres, telefoonnummer,…).
- Je kunt deze gegevens niet zomaar **verwerken** (verzamelen, raadplegen, wijzigen, gebruiken, verspreiden, vernietigen,…). In principe dienen de personen van wie je gegevens verwerkt hiervoor expliciet toestemming te geven. In het kader van een wettelijke verplichting (bv. afleveren van een identiteitskaart), bij de uitvoering van een overeenkomst (bv. reservatie van een zaal) of bij de uitvoering van het openbaar gezag mag je ook persoonsgegevens verwerken. Wees vooral voorzichtig bij het verwerken van **gevoelige persoonsgegevens** (bv. medische of juridische gegevens). Bij twijfel vraag je best advies aan de DPO.

- Wees **transparant** bij de verwerking van persoonsgegevens (leg uit waarom je de persoonsgegevens verzamelt en wat je ermee doet), gebruik de persoonsgegevens alleen waarvoor je ze verzamelde, verwerk alleen de gegevens die je echt nodig hebt, bewaar de gegevens niet langer dan nodig en behandel persoonsgegevens **vertrouwelijk**.
- Het **verstrekken** van persoonsgegevens **aan derden** is in principe niet toegelaten. Krijg je een dergelijke vraag, leg deze dan eerst ter advies voor aan de DPO.
- Gebruikers die persoonsgegevens verwerken moeten er zich van bewust zijn dat dergelijke verwerkingen gelogd worden (waaronder identificatie van de persoon die de verwerking uitvoert, identificatie van de persoon voor of over wie de verwerking wordt uitgevoerd, datum en tijdstip, reden van de verwerking). Het gaat om een verplichting, opgelegd door diverse overheden of overheidsinstanties (bijv. voor consultaties rijksregister, KSZ enz.). De DPO is bevoegd om steekproeven te houden op deze raadplegingen.

Beroepsgeheim en behandelen vertrouwelijke informatie

Onverminderd de wettelijke regels inzake beroepsgeheim waaraan de gebruiker onderworpen is, is elke gebruiker ertoe gehouden alle kennis en gegevens, zowel betrekking hebbende op burgers als op andere confidentiële gegevens, die hij in het kader van zijn werkzaamheden ten behoeve van de werkgever heeft verworven of mocht verkrijgen, zowel tijdens als na deze werkzaamheden, strikt geheim te houden. Bij twijfel of iets onder het beroepsgeheim of onder vertrouwelijke informatie valt, richt de gebruiker zich tot de hiërarchische lijn.

Vertrouwelijke bedrijfsgegevens en persoonsgegevens worden nooit ter beschikking gesteld van derden, behalve wanneer een dergelijke doorgifte wordt opgelegd door of krachtens een wet, decreet of andere regelgeving.

Ook na het beëindigen van de arbeidsovereenkomst blijft de gebruiker gebonden door het beroepsgeheim.

Openbaarheid van bestuur versus vertrouwelijke informatie

Lokale overheden beschikken over een veelheid aan informatie. Veel van die informatie wordt ter beschikking gesteld van de burger in het kader van de openbaarheid van bestuur. Dit wil echter niet zeggen dat vertrouwelijke informatie zomaar gedeeld kan worden omdat dit kan conflicteren met:

- belangen van natuurlijke personen, bijvoorbeeld gegevens die onder het medische geheim vallen, tuchtdossiers, dossiers met persoonsinformatie;
- belangen van de werkgever, bijvoorbeeld het geheim van beraadslagingen van instanties die politieke beslissingen nemen, informatie over een interne audit;
- belangen binnen gerechtelijke procedures, bijvoorbeeld informatie met betrekking tot gerechtelijke procedures of strafrechtelijke feiten waarbij de werkgever betrokken partij is;
- zaken van maatschappelijk belang, bijvoorbeeld informatie die invloed kan hebben op de openbare orde en veiligheid of informatie die een economisch, financieel of commercieel belang kan schaden.

De gebruiker denkt na over het soort van informatie waarover hij beschikt en hij verspreidt de informatie alleen als hij er zeker van is dat het niet over vertrouwelijke gegevens gaat en niet in strijd is met de regelgeving inzake openbaarheid van bestuur. Bij twijfel neemt de gebruiker onmiddellijk contact op met de hiërarchische lijn.

Meer informatie is terug te vinden in het schema “Openbaarheid van bestuur versus privacy”. Dit document is raadpleegbaar in de publieke map op de server of kan opgevraagd worden bij de DPO.

Meldplicht datalekken en beveiligingsincidenten

Gebruikers die datalekken of beveiligingsincidenten vaststellen dienen deze te melden aan de DPO (privacy@mesen.be). Indien het gaat om IT-gerelateerde incidenten worden deze eveneens aan de externe IT’er gemeld.

- Een **incident** is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of

informatieverwerkende systemen in gevaar is of kan komen (bijvoorbeeld besmettingen met virussen, diefstal van een laptop, enz.).

- Een **datalek** is het gevolg van een beveiligingsincident, waarbij persoonsgegevens verloren zijn gegaan of niet is uit te sluiten dat persoonsgegevens onrechtmatig in handen van derden zijn gevallen (bijv. blootstelling van persoonsgegevens via een lek in de website).

Meer informatie is terug te vinden in het schema “Melden van incidenten en datalekken”. Dit document is raadpleegbaar in de publieke map op de server of kan opgevraagd worden bij de DPO.

Richtlijnen met betrekking tot controlerecht

Recht op 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 dienst IT en de DPO mogen 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.

Hoe kan er worden gecontroleerd?

Permanente algemene controle: hieronder vallen o.m. het al dan niet automatisch monitoren van de IT systemen en informatie of het niet-geïndividualiseerd (laten) controleren i.f.v. de veiligheid, performantie en goede werking van de IT-systemen.

Occasionele algemene controle: Het monitoren en controleren van IT gebruik bij een beperkte groep personeelsleden voor een bepaalde periode. Bij deze controles worden volgende punten bekeken zonder individuele identificatie:

- Lijst van bezochte websites of geraadpleegde informatie, de frequentie, tijdstip en duur van deze bezoeken en het volume van informatie dat wordt bewaard of getransfereerd.
- Het volume en aantal uitgaande e-mails

Individuele controle: controleert gelijkaardige punten als de occasionele algemene controle, maar op een geïndividualiseerde manier. Deze vorm van controle is (enkel) toestaan indien:

- Uit occasionele algemene controle blijk dat één of meerdere personeelsleden uit de gecontroleerde groep de IT-middelen niet hebben gebruikt conform de voorliggende afspraken.
- Indien uit een permanente of occasionele controle blijkt dat een gebruiker de veiligheid, performantie en/of goede technische werking van de ICT-systemen in het gedrag brengt of de kosten abnormaal hoog doet oplopen. In deze gevallen kan er direct geïndividualiseerd worden gecontroleerd en nagegaan wie de betrokken gebruiker(s) is/zijn.
- De betrokkene dient niet vooraf te worden gewaarschuwd en er kan meteen een geïndividualiseerde controle worden uitgevoerd indien er een gegrond vermoeden bestaat van ernstige onregelmatigheid of inden het personeelslid zich schuldig maakt aan:
  - Ongeoorloofde of lasterlijke feiten, of feiten die strijdig zijn met de goede zeden of die de waardigheid van een ander persoon kunnen schaden.
  - Openbaar maken van vertrouwelijke informatie.
  - Feiten die de veiligheid, performantie of de goede technische werking van de IT-systemen in het gedrang brengen.
- Conform de wet is de werkgever verplicht tot onderzoek bij feiten van geweld, pesterijen en ongewenst seksueel gedrag. De algemeen directeur is hierbij bevoegd om direct geïndividualiseerd te controleren. Voor dit doel kunnen ook gegevens worden gecontroleerd die in het verleden zijn ontstaan.
- In de andere gevallen zal de individuele controle zal pas worden uitgevoerd nadat:

- Betrokkene(n) op een duidelijke en begrijpelijke wijze werden ingelicht over het bestaan van een onregelmatigheid
- En nadat het personeel op de hoogte werd gebracht dat er geïndividualiseerd zal worden gecontroleerd n.a.v. het vaststellen van deze onregelmatigheid.

Sancties

Bij het vaststellen van ongeoorloofd gebruik van IT-middelen kunnen sancties worden opgelegd conform het arbeidsreglement of de toepasselijke regelgeving.