BIJLAGE 8 – BELEID BETREFFENDE HET GEBRUIK VAN DE TER BESCHIKKING GESTELDE INFORMATICA- EN COMMUNICATIEMIDDELEN

BIJLAGE BIJ HET ARBEIDSREGLEMENT

Artikel 1. Doel en toepassingsgebied

Het bestuur stelt aan zijn personeelsleden een aantal communicatiemiddelen zoals e-mail, internet, laptop, GSM en telefoon ter beschikking in het kader van de uitoefening van hun functie. Het gebruik van deze middelen door de personeelsleden wordt aangemoedigd aangezien deze kunnen bijdragen tot de verhoging van de kwaliteit van hun prestaties en de geleverde dienstverlening. Hierbij heeft het bestuur wettelijke en morele verplichtingen tot het nemen van veiligheidsmaatregelen. Het is dan belangrijk dat personeelsleden een eenduidig verstaanbaar document kunnen raadplegen rond het gebruik van deze middelen.

De hierna vastgelegde policy is van toepassing op alle door het bestuur ter beschikking gestelde middelen, dit kan omvatten:

- Elektronische communicatiemiddelen (o.m. telefoon, GSM, fax, smartphone, e-mail, interne memosystemen, internet, toets- en leerplatformen, administratieve systemen, informatiesystemen, …)
- ICT-middelen, IT-infrastructuur (o.m. PC/laptop, tablet, modems, netwerkprogrammatuur, interne en externe netwerken, LAN, informatica- en softwaresystemen, …)
- Alle gegevens die worden verzonden of worden opgeslagen.

Deze bijlage aan het arbeidsreglement heeft als doel duidelijke afspraken te maken betreffende het gebruik van deze communicatiemiddelen, waarbij een goede balans wordt nagestreefd tussen het verantwoord gebruik van deze middelen en de bescherming van de privacy van de personeelsleden.

Het is van toepassing op alle categorieën van personeelsleden en stagiairs die rechten hebben tot informatie en informatiesystemen van het bestuur. Deze bijlage is eveneens van toepassing indien de gebruiker zijn eigen communicatiemiddelen gebruikt, in combinatie met deze van het bestuur, b.v. gebruik van het professioneel e-mailadres op een eigen computer thuis en/of smartphone.

Artikel 2. Verantwoordelijkheden van de gebruiker

De middelen die aan het personeelslid of elke andere gebruiker ter beschikking worden gesteld, blijven eigendom van het bestuur.

Iedere medewerker dient zich te gedragen als een goede huisvader/-moeder, draagt zorg voor de middelen die hem/haar ter beschikking zijn gesteld. Deze middelen worden gebruikt op een professioneel, sociaal, ethisch en juridisch correcte wijze, overeenkomstig de bepalingen die hier zijn opgenomen en de instructies die ter zake worden gegeven.

De gebruiker heeft, voor zover van toepassing, een aantal verantwoordelijkheden en plichten aangaande:

1. Het **gebruik** van de middelen:
    - In goede toestand bewaren van de middelen die ter beschikking gesteld werden.
    - Niet onbeheerd achterlaten van de ter beschikking gestelde middelen en het nemen van voldoende veiligheidsmaatregelen om diefstal ervan te verhinderen.
      Bijvoorbeeld:
        - *het afsluiten van het gebouw/lokalen als men als laatste vertrekt*
        - *wegbergen mobiele toestellen die niet in gebruik zijn (tablets/smartphones)*
        - *documenten mogen niet worden achtergelaten bij printers, kopieertoestellen, …*
    - Nemen van voldoende veiligheidsmaatregelen die de mogelijkheid tot diefstal van informatie zo klein mogelijk maakt.
      Bijvoorbeeld:
        - het activeren van de schermbeveiliging van het werkstation/laptop (CTRL-ALT-DELETE en vervolgens 'vergrendelen'), smartphone, … (op iedere pc moet een schermbeveiliging met wachtwoord ingesteld zijn zodanig dat deze na maximaal 10 minuten inactiviteit in werking treedt).
        - op het einde van de werkdag dient het werkstation, laptop, smartphone, … te worden afgesloten,
        - het niet ter beschikking stellen van mail/agenda aan apps/applicaties buiten het intern netwerk (wordt vaak door apps/applicaties automatisch gevraagd).

2. De **veiligheid van de gegevens** die bewaard worden op de systemen:
    - Alle gegevens op de netwerken worden dagelijks geback-upt. Gegevens op lokale schijven/portables worden NIET geback-upt. Deze laatste gegevens vallen volledig onder uw verantwoordelijkheid.
    - Het is verboden om de geïnstalleerde virusscanner uit te schakelen tenzij in zeer uitzonderlijke gevallen na uitdrukkelijke toestemming van de dienst ICT.
    - Geconfronteerd met een virus, een verdachte e-mail of een verdacht document, moet dit onmiddellijk gemeld worden aan de dienst ICT, die verder de nodige maatregelen neemt om verdere schade te verhinderen.
    - Incidenten, eventuele lacunes in de beveiliging van het computersysteem of van methodes die de beveiliging van de gegevens in het gedrang brengen mogen niet aan derden gemeld worden; het uitbuiten van deze zwakheden wordt beschouwd als (poging tot) inbraak. Ook deze moeten onmiddellijk gemeld worden aan de dienst ICT.

- Elke gebruiker van een persoonlijk e-mail account van het bestuur dient op regelmatige tijdstippen zijn/haar berichten te lezen, op te ruimen en eventueel zijn/haar postbus te archiveren.
- Opslaan van gegevens voor doeleinde van het bestuur moeten bewaard worden op de daarvoor voorziene IT-infrastructuur en volgens de voorziene structuur en niet op de lokale harde schijven of eigen toestellen en media (bestanden worden dus steeds opgeslagen op de netwerkdrive en niet op de harde schijf zijnde de C-schijf).
- Op het werkstation mag enkel gewerkt worden met officieel geïnstalleerde soft- en hardware. Het verbinden met het netwerk van niet tot het officiële IT-infrastructuur behorende hardware is verboden.
- Het gebruik van fysieke gegevensdragers voor de opslag van vertrouwelijke gegevens (zoals cd's, USB-sticks, lokale of draagbare harddisks, …) is niet toegestaan. Enkel voor de back-up procedure en indien de verantwoordelijke dagelijks bestuur uitdrukkelijk de toestemming geeft om toch vertrouwelijke of persoonsgegevens op een draagbare gegevensdrager te bewaren kan hierop een uitzondering worden gemaakt. Deze gegevensdragers moeten dan wel steeds op een veilige plek bewaard worden en indien mogelijk geëncrypteerd of met wachtwoord beveiligd zijn.
- Media die niet meer gebruikt worden en die vertrouwelijke informatie of persoonsgegevens bevatten, moeten met speciale zorg behandeld worden. Bij vernietiging en eventueel hergebruik ervan moet erop gelet worden dat alle vertrouwelijke informatie wel degelijk verdwenen is.
- Hardware die geen eigendom is van het bestuur mag enkel na uitdrukkelijke toestemming van de dienst ICT worden verbonden met de IT-infrastructuur van het bestuur. Dit omvat onder meer externe harde schijven, USB-sticks, digitale camera's, tablets, smartphones, USB-modems, ….
- Software mag alleen door de dienst ICT of in diens opdracht worden gedownload en geïnstalleerd. Indien blijkt dat bepaalde toepassingen op werkstations werden geïnstalleerd zonder overleg met de dienst ICT, kan deze – na samenspraak met de algemeen directeur – de programma's verwijderen.
- Het kopiëren van software binnen de IT-infrastructuur van het bestuur is niet toegestaan.

3. **Omgaan** en **doorgeven** van **persoonsgegevens**:
   - Persoonsgegevens verkregen uit een **authentieke bron** (zoals het bevolkings-, rijksregister, KSZ, …) mogen enkel worden geconsulteerd en bewerkt in het kader van wettelijke opdracht(en), deze omvatten onder andere:
     - Het toekennen van vergunningen, rechten, diensten en voordelen hetzij op initiatief van de betrokkenen zelf, hetzij proactief op basis van een bepaalde bevoegdheid.
     - Het vestigen en innen van belastingen, retributies en schuldvorderingen, het opleggen van maatregelen in het kader van de handhavingsbevoegdheid waarover een lokaal bestuur beschikt.

- Het informeren en communiceren, in het kader van de juiste bevoegdheden met het oog op een efficiënt en effectief klantenbeheer van het bestuur.
- Het verkrijgen van basisgegevens uit een authentieke bron voor het opstellen van een omgevingsanalyse in functie van de algemene beleidsplanning en budgetopmaak, en in functie van een aantal specifieke planningsnoden - Personeelsbeheer - …

- Persoonsgegevens verkregen binnen het uitvoeren van een functie mogen op **geen enkele manier extern worden verspreid of meegedeeld aan derden** (behalve indien de mededeling(en) noodzakelijk is (zijn) in het kader van de uitvoering van een wettelijke bevoegdheid) en conform de wet verwerking persoonsgegevens (8 dec 1992) en Algemene Verordening Gegevensbescherming (AVG van kracht sinds 25 mei 2018).
- Persoonsgegevens worden **niet onbeveiligd** via e-mail doorgegeven.
- Persoonsgegevens worden niet **via onbeveiligde externe media** doorgegeven.
- Persoonsgegevens worden **niet opgeslagen op systemen buiten het bestuur** (bv Dropbox, WeTransfer, …).

4. Het bestuur behoudt zich het recht voor om op elk ogenblik de toegang tot bepaalde of alle sites te verbieden, waarvan de inhoud onwettig, beledigend of onaangepast zou zijn of meer in het algemeen vreemd zou zijn aan de activiteiten van de personeelsleden. Betreffende het gebruik van internet zijn expliciet verboden:
   - het downloaden en installeren van eender welke software, software-updates of zogenaamde plug-ins;
   - het downloaden van materiaal dat in overtreding is met de bestaande wetgeving op de auteursrechten;
   - het downloaden of raadplegen van audio- of videobestanden, ongeacht de verspreidingsvorm ervan (b.v. mp3, divx, avi, streaming audio, …), tenzij dit een expliciet onderdeel is van de functieomschrijving van het personeelslid;
   - het gebruik van het internet om informatie die een nadelig effect kan hebben op de reputatie of de goede naam van het bestuur, haar personeelsleden of derden, op te zoeken, te visualiseren, te downloaden of te verspreiden;
   - het deelnemen aan discussieforums, chatrooms of nieuwsgroepen zonder een gewettigd professioneel doel;
   - het bewust consulteren van erotische, pornografische, racistische, discriminerende, beledigende en aanstootgevende websites, zelfs indien het gaat om wettelijk toegelaten publicaties;
   - het trachten in te breken in een computer, database of netwerk;
   - via internet onethisch of in strijd met de wet handelen;
   - … (deze lijst is ongelimiteerd).

Uitzondering geldt aan de personeelsleden van de Bibliotheek, waarbij toelating wordt gegeven tot het installeren van databanken e.d. die aldus door de burgers kunnen geraadpleegd worden.

- Contacteer de IT-verantwoordelijke indien je nood hebt aan additionele software;
- Verander niet zelf de standaard configuratie;
- Software is wettelijk beschermd tegen illegaal gebruik. Het stadsbestuur Borgloon zal de benodigde licenties aankopen, indien uw aanvraag ontvankelijk verklaard is. Alle softwarelicenties worden beheerd door de IT-verantwoordelijke;
- Verwittig de IT-verantwoordelijke indien je een bepaald softwarepakket niet meer nodig hebt. Deze licentie kan misschien gebruikt worden door een collega ofwel kan het onderhoud opgezegd worden en komen middelen vrij voor andere behoeften.

5. Het omgaan met bestanden van onbekende oorsprong én bij twijfel contact opnemen met de dienst ICT:
    - B*ijvoorbeeld:*
        - *Verdachte bijlagen in e-mails niet openen*
        - *Onbekende gedownloade bestanden niet openen*
        - *Onbekende links niet openen*

6. Het elektronisch communiceren met anderen in een professionele uitwisseling moet voldoen aan de hierna volgende voorwaarden:
    - correct vermelden van: naam en functie van het personeelslid, naam bestuur, het gebruikelijke telefoonnummer, overeenkomstig de huisstijl
    - indien gebruik van e-mail, dient elk bericht de volgende disclaimer te bevatten (uitgeschreven of verwijzend naar een URL met deze inhoud): "*Dit bericht met zijn eventuele bijlage(n) verbindt het bestuur van Borgloon niet, noch kan het bestuur aansprakelijk worden gesteld voor de inhoud ervan.*"

    Zijn expliciet verboden:
    - het verspreiden van vertrouwelijke informatie m.b.t. de werkgever, zijn commerciële partners of de werknemers, tenzij dit vereist is voor de werkzaamheden van de werknemer in het kader van de arbeidsovereenkomst en, in dat geval, rekening houdend met de verbintenissen van geheimhouding die door het gemeentebestuur desgevallend onderschreven werden;
    - het verspreiden van gegevens beschermd door het auteursrecht, in strijd met de wetten die het auteursrecht beschermen;
    - het "doorsturen" van elektronische boodschappen zonder gewettigd professioneel doel, in omstandigheden die nadeel kunnen berokkenen aan de auteur van het oorspronkelijke bericht;
    - elk gebruik van e-mail dat van aard is om de waardigheid van anderen in het gedrang te brengen, meer bepaald het verzenden van boodschappen inzake ras, nationaliteit, geslacht, seksuele geaardheid, leeftijd, handicap, geloof of politieke overtuiging van een persoon of een groep van personen;
    - het gebruik van e-mail in het kader van een professionele activiteit die vreemd is aan de arbeidsovereenkomst van de werknemer met de werkgever;
    - deelname aan "kettingbrieven";
    - het verzenden van provocerende e-mails;

- het gebruik van e-mail om bepaalde situaties binnen de onderneming openlijk aan te klagen;
- het verzenden van e-mail waarin wordt aangezet tot het plegen van strafbare feiten;
- het verzenden van berichten die een publiciteit inhouden voor diensten van seksuele aard;
- het verzenden van berichten die beschouwd worden als pornografisch, van welke aard ook;
- het verzenden van berichten die een racistische of xenofobe boodschap inhouden of die als discriminerend, seksistisch, obsceen, pornografisch, belasterend of bedreigend kan beschouwd worden;
- het verzenden van berichten die verband houden met spelen en weddenschappen, verdovende middelen of vormen van fraude.
- meer in het algemeen, elk gebruik van het e-mail systeem in het kader van een onwettige activiteit, welke ook;
- **Gebruik niet het gemeentelijk e-mail adres om grappen en rommelboodschappen te verspreiden (noch intern, noch extern). Er gaat heel wat kostbare tijd verloren met dergelijke mails. Tijd die door het bestuur betaald wordt.**
- … (deze lijst is ongelimiteerd).

Bij twijfel aangaande de geoorloofdheid van het gebruik van e-mail dient de werknemer zich te wenden tot zijn/haar rechtstreekse overste.
Indien het e-mail systeem gebruikt wordt door werknemersvertegenwoordigers in het kader van de uitoefening van hun syndicale activiteiten, dient rekening te worden gehouden met de ter zake geldende gedragsregels. De werknemersvertegenwoordigers en de werkgever maken verdere afspraken omtrent het gebruik van e-mail voor de uitoefening van de syndicale activiteiten.

7. Ingeval van afwezigheid (vakantie, ziekte, etc.) dienen de nodige afspraken te worden gemaakt met het diensthoofd inzake de opvolging van de binnenkomende e-mails. Op je eigen e-mail adres dient er een afwezigheidsbericht ingesteld te worden: “Ik ben afwezig van … tot … Dringende berichten kan je zolang sturen aan … “(algemeen e-mailadres van de dienst of het e-mailadres van een collega).

   Laat het algemene e-mailadres van je dienst (indien aanwezig) niet zonder beheerder tijdens een vakantieperiode. Als de persoon die verantwoordelijk is voor de het algemene e-mailadres met vakantie is, moet steeds een collega deze mails opvolgen.

   De werknemer gaat ermee akkoord dat in geval van een plotse gebeurtenis zoals ongeval, ziekte …. de systeembeheerder de binnengekomen e-mails hetzij mag doorsturen naar een collega (deze instelling gebeurt via de server, dus zonder inzage van de mailbox), hetzij de mailbox mag inkijken teneinde de afzender tijdig een

antwoord te kunnen sturen (deze keuze zal de werknemer kenbaar kunnen maken bij de ondertekening van de verklaring tijdens het onthaalgesprek).

Artikel 3. Wachtwoorden en loginnamen

Elke loginnaam moet beschermd worden met een sterk gekozen wachtwoord. **Toegang** tot de IT-infrastructuur, het netwerk, softwarepakketten, interne en externe platformen wordt verleend door **individuele authenticatie**.

Voor wachtwoorden gelden de volgende regels:

- Uw login-ID heeft volgend formaat: Eerste letter van uw voornaam gevolgd door de eerste letter van uw familienaam. In het geval van conflict zullen speciale afspraken gemaakt worden.
- Wachtwoorden dienen minimum 8 karakters te beschikken, liefst gecombineerd met een cijfer. Kies nooit familienamen, leesbare woorden of een cijfercombinatie. Deze zijn gemakkelijk te kraken door middel van gespecialiseerde tools.
- Wachtwoorden dienen regelmatig gewijzigd te worden en in elk geval onmiddellijk als dit door de dienst ICT gevraagd wordt (*bijvoorbeeld na vaststelling van een inbraak of wanneer het wachtwoord te zwak is*) of als de gebruiker een vermoeden heeft dat het niet meer geheim is.
- Niemand mag zijn/haar wachtwoord aan derden doorgeven (bv. collega's, jobstudenten, stagiairs, consulenten, …) en/of door derden laten gebruiken en niemand mag de loginnaam van een ander gebruiken.
- Wachtwoorden van anderen proberen te kraken of te achterhalen is verboden.
- Het is niet toegelaten om wachtwoorden onbeveiligd op te slaan of zichtbaar (*bijvoorbeeld Post-it*) rond te laten slingeren.
- Er dient omzichtig omgegaan te worden bij het ingeven van wachtwoorden (*bijvoorbeeld niet als iemand toekijkt*).
- Iedere gebruiker is verantwoordelijk en aansprakelijk voor alles wat onder zijn/haar loginnaam (gebruikersidentificatie) en wachtwoord gebeurt. Toegangsrechten worden verleend na goedkeuring, enerzijds wordt dit beslist door de "pakket/software-verantwoordelijke" (hiërarchisch hogere) en uitgevoerd door de technische verantwoordelijke. Het is de "pakket/software-verantwoordelijke" (hiërarchisch hogere) die bij elke in- en uitdiensttreding verantwoordelijk is voor het toekennen/afnemen van deze rechten (PIPOPC formulier). Algemeen beogen we need-to-know in plaats van nice-to-know. Hierbij krijgt een (interne en externe) gebruiker standaard enkel de toegangsrechten die noodzakelijk zijn voor de functionele rol van de gebruiker binnen de organisatie.

Wanneer men merkt dat men toegang heeft tot informatie waarvoor men niet gemachtigd zou moeten zijn, moet de werknemer dit onmiddellijk melden bij de "pakket/softwareverantwoordelijke" (hiërarchisch hogere) zodat de toegangen beperkt kunnen worden.

Artikel 4. Interne richtlijnen inzake e-mail gebruik

E-mailberichten kennen een groot aantal verschijningsvormen. Een bericht kan een officiële brief vervangen, maar evengoed een telefoongesprek of een post-it briefje. Het is steeds aan jou als ontvanger om de aard van een inkomend bericht in te schatten en er het gepaste gevolg aan te geven.

Hieronder wordt beschreven welk type berichten in ieder geval uit naam van het schepencollege een antwoord moeten krijgen en welke berichten je in eigen naam kan antwoorden.

1. Berichten die je zelf kan antwoorden:
   - Vragen om operationele informatie: openingsuren, vragen voor het toezenden van folders of brochures, inschrijvingen voor evenementen, e.d.
   - Correspondentie met collega's bij andere besturen

2. Volgens het klassieke procesverloop:
   - Inkomende berichten die betrekking hebben op het gevoerde beleid van het gemeentebestuur krijgen altijd een formeel antwoord van het college.
   - Berichten waarbij de afzender een klacht instuurt over dienstverlening van het gemeentebestuur.
   - Alle bezwaarschriften

   Deze berichten dienen doorgestuurd te worden naar postbeheer@borgloon.be . Aan de afzenders verzend je een ontvangstbevestiging, *bijvoorbeeld "Wij hebben uw bericht goed ontvangen. Uw bericht werd bezorgd aan het college van burgemeester en schepenen".*

3. Worden doorgestuurd naar postbeheer@borgloon.be :
   - Alle schriftelijke vragen van de pers;
   - Alle vragen dienen doorgestuurd te worden naar postbeheer@borgloon.be .

Inzake de **opmaak** van e-mails gelden er volgende regels:

- Vul steeds het onderwerpveld in. Veel e-mailgebruikers negeren berichten zonder onderwerp.
- Behalve voor informele berichten gebruik je steeds een correcte en zo volledig mogelijke aanspreking: "Geachte heer Jansens", "Geachte mevrouw Peeters" …
- Gebruik een volledige en uniforme ondertekening:

Voornaam Naam
Functie
E voornaam.naam@borgloon.be
T 012 67 xx xx

Administratief centrum 'Kanunnikenhuis'
Speelhof 10, 3840 Borgloon
www.borgloon.be

Interne afspraken omtrent het beantwoorden van e-mails:

- Beantwoord een e-mailbericht zo snel mogelijk. Als je niet onmiddellijk kan antwoorden, stuur dan een ontvangstbevestiging waarin je vermeldt wanneer je correspondent een definitief antwoord krijgt.
- Blijf steeds hoffelijk, ook in antwoorden op brutale berichten.
- Maak nooit opmerkingen over personen, enkel over onderwerpen.
- Wees voorzichtig met symbolen, kleuren en speciale tekens. Deze zijn bij de ontvanger misschien niet leesbaar.

Medewerkers dienen extra waakzaam te zijn voor:

1. Virussen

De IT-verantwoordelijke zal er zorg voor dragen dat de virusscan dagelijks wordt geüpdate Dit neemt echter niet weg dat een virus zich zo snel kan verspreiden en dit vooraleer de dagelijkse update gebeurd is. Neem dus de hiernavolgende regels goed in acht.

- Laat uw NIEUWSGIERIGHEID VAREN en open niet zomaar klakkeloos elke e-mail;
- Mailtjes waarvan de afzender u onbekend is of waarvan het onderwerp in een andere taal dan het Nederlands staat behandelt u met de nodige omzichtigheid. Verwittig liever eerst de IT-verantwoordelijke vooraleer de mail te openen;
- Hou de mogelijkheid van een virusinfectie open wanneer iets "plezant" gebeurt met de computer;
- Volg steeds de richtlijnen van de IT-verantwoordelijke. Het vergt veel meer werk om een geïnfecteerd netwerk terug operationeel te krijgen dan dat u een mailtje verwijdert. Iemand die u echt wil bereiken en merkt dat u niet reageert, zal u wel via een andere weg proberen te bereiken.

2. Kettingmails en hoaxen

Ga nooit in op verzoeken om een bericht naar je hele adresboek door te sturen. Meestal gaat het om hoaxen, valse viruswaarschuwingen. Stuur dergelijke berichten door naar de

systeem- beheerder die zal beslissen of er al dan niet bijkomende maatregelen dienen genomen te worden.
Kettingmails hebben meestal slechts één doel: het verzamelen van zoveel mogelijk werkende e-mailadressen. Deze worden later gebruikt voor spamming (ongevraagd toesturen van reclamemails) of voor het verspreiden van virussen.

Artikel 5. Interne richtlijnen inzake GSM/smartphone gebruik

A. Toepassingsgebied

Voor de toepassing van dit reglement wordt verstaan een mobiele telefoon die door de gemeente ter beschikking van het personeelslid wordt gesteld ter uitvoering van zijn/haar taken. Het wordt beschouwd als een werkmiddel. De gemeente koopt de telefoon aan en neemt de bijhorende kosten op zich. De toewijzing van een individuele mobiele telefoon gebeurt aan de personeelsleden die steeds bereikbaar moeten zijn binnen de diensturen (en hiervoor niet steeds over een vaste telefoon kunnen beschikken) en buiten de diensturen in functie van een opdracht.

B. Kostprijs en gebruik van de gsm van de gemeente

Het college van burgemeester en schepenen of het vast bureau bepaalt op basis van de noodzakelijke functionaliteiten welke telefoon aangeschaft zal worden tegen welke kostprijs.

De mobiele telefoon van de gemeente kan niet ter beschikking worden gesteld van derden.

Bij twijfel over de facturatie voor werkdoeleinden kan er aan het betrokken personeelslid worden gevraagd om hierover meer toelichting te verstrekken.

C. Schade en verlies van de gsm van de gemeente

Een mobiele telefoon van de gemeente dient met de nodige zorg behandeld (bewaren op een droge plaats, …) en mag niet onbeheerd worden achtergelaten. Alleen onder deze omstandigheden zal de gemeente de kosten voor schade en verlies op zich nemen.

Bij schade, verlies of diefstal zal dit steeds gemeld worden aan het bestuur. Bij diefstal wordt steeds aangifte gedaan.
De werknemer is volledig verantwoordelijk voor het gebruik en bewaring van zijn eigen mobiele telefoon. Verlies of beschadiging – zelfs tijdens de diensturen – wordt niet vergoed door de gemeente.

D. Gebruikstermijn

Bij aanvang van het gebruik ondertekent het personeelslid deze richtlijnen voor akkoord.

Indien een personeelslid afwezig is (wegens ziekte, loopbaanonderbreking, vakantie,….) en het nummer van de mobiele telefoon gebruikt wordt voor opdrachten, zal hij zijn mobiele telefoon overhandigen aan zijn vervanger voor het vervullen van de taken.

Bij het beëindigen van de arbeidsrelatie of bij het stopzetten van de opdrachten waarvoor de mobiele telefoon ter beschikking wordt gesteld, zal het personeelslid de mobiele telefoon terugbezorgen aan de gemeente. Indien het personeelslid de mobiele telefoon niet terug overhandigt, zal hij de kostprijs betalen die berekend wordt op de afschrijving van de mobiele telefoon: per maand wordt er 1/36ste van de aankoopprijs in mindering gebracht. De minimale kostprijs is 1/36ste van de aankoopprijs.

De levensduur van een telefoon wordt op 36 maanden vastgelegd. Indien een personeelslid dit wenst, kan hij de door hem gebruikte telefoon overnemen van de gemeente bij beëindiging van de arbeidsovereenkomst of bij aankoop van een nieuwe mobiele telefoon door de gemeente. De kostprijs hiervan wordt berekend op de afschrijving van de mobiele telefoon: per maand wordt er 1/36te van de aankoopprijs in mindering gebracht. De minimale overnameprijs is 1/36ste van de aankoopprijs.

E. Afrekening – Voordeel van alle aard (VAA)

Overeenkomstig het Koninklijk Besluit van 2 november 2017 tot wijziging van het KB/WIB 92, op het stuk van de voordelen van alle aard voor het persoonlijk gebruik van een kosteloos ter beschikking gestelde PC, tablet, internetaansluiting, mobiele telefoon of vast of mobiel telefoonabonnement:

Het privégebruik van een GSM/smartphone is een voordeel in natura dat moet geraamd worden op 3 EUR per maand.

Het privégebruik van het telefoonabonnement is een voordeel in natura dat moet geraamd worden op 4 EUR per maand.

Het privégebruik van het internet (dataverkeer) moet geraamd worden op 5 EUR per maand.

F. Mobiele betalingen

Mobiele betalingen – bijvoorbeeld sms-parking of tickets van De Lijn – zijn standaard toegelaten, maar worden standaard altijd aangerekend op de privéfactuur. Als dit om een werk gerelateerde betaling gaat, kan deze worden teruggevorderd via een terugvorderingsnota.

G. Bellen in het buitenland (buiten de EU-roaming)

Roaming betekent dat je met jouw mobiel toestel kan bellen en oproepen ontvangen als je in het buitenland bent. De tarieven zijn verschillend van land tot land. Zelf bellen, data downloaden of gebeld worden in het buitenland kost erg veel en doet de factuur ernstig

stijgen en worden aangerekend op de privéfactuur. Binnen de EU gelden de binnenlandse tarieven.

H. Privacy

Het bestuur zal de inhoud zelf van de communicatie op de bedrijfs- of dienst-gsm nooit bekijken of beluisteren. Het bestuur is gemachtigd om de gegevens rond de communicatie (dus niet de inhoud van de communicatie) zoals bijvoorbeeld het aantal gesprekken, de bestemming van de gesprekken en duurtijd te bekijken en bij kennelijk misbruik de gepaste maatregelen te nemen.

I. Rapportering, controle en evaluatie

De diensten moeten het correcte gebruik en verbruik van de gsm's bewaken via rapportering, controle en evaluatie. Bij een vermoeden van sterk afwijkend verbruik vraagt de leidinggevende het akkoord van de algemeen directeur om de bestemming, duur en tijdstip van de gesprekken te kunnen nakijken.

Artikel 6. Algemene veiligheid

- Verplaats nooit een desktop computer op je eentje, consulteer de IT-verantwoordelijke;
- Zorg er altijd voor dat de luchtaanvoer en –uitvoer van de computerapparatuur vrij is (geen ventilatiesystemen afplakken of de ventilatie versperren door andere apparatuur).
- Plaats nooit voedsel of drank in de buurt van de computer. Nuttig nooit je maaltijd boven je klavier.

Artikel 7. Persoonlijk gebruik

In de mate dat privégebruik van communicatiemiddelen (e-mail, internet, telefoongebruik, …) is toegestaan, moet dit gezien worden als een gunst en niet als een recht. Onder toegelaten persoonlijk gebruik van middelen binnen redelijke perken wordt onder andere verstaan dat:

- het netwerk niet te veel belast mag worden door internetverkeer
- anderen door dit gebruik niet mogen gestoord worden bij de uitoefening van hun beroepsactiviteiten,
- er behoudens andere afspraken geen kosten aan verbonden zijn voor de organisatie,
- het persoonlijke gebruik van de middelen geen nadelige invloed heeft op de individuele arbeidsprestaties volgens het overeengekomen arbeidsrooster,
- er niet wordt ingeschreven op persoonlijke nieuwsbrieven met het professioneel emailadres,
- uitgaande privémail krijgt in "onderwerp" de duidelijke vermelding "PRIVÉ". De inkomende privé-mail wordt (indien hij wordt bewaard) duidelijk in een PRIVE-map opgeslagen. Deze map zal de naam "PRIVÉ" dragen en bevindt zich op de C-schijf. De map mag de 500MB niet overschrijden.

- gebruik professioneel mailadres in kader van privé aangelegenheden mag geen verwijzing hebben naar het bestuur, dit wil zeggen dat de officiële handtekening niet mag worden gebruikt.

Het bestuur heeft het recht om, wanneer dit om bedrijfsredenen vereist is of wanneer dit wettelijk bepaald is:

- de voorwaarden voor het ter beschikking stellen van ICT-middelen te herzien en eventueel te beperken,
- de gemaakte kosten voor persoonlijk gebruik op de gebruiker te verhalen,
- de verloren arbeidstijd aan te rekenen.

Artikel 8. Controle

Binnen de wettelijke grenzen kan het bestuur controle uitoefenen op informatie die een gebruiker opslaat, verspreidt, verstuurt of ontvangt binnen het toepassingsgebied van deze bijlage aan het arbeidsreglement en/of op informatiesystemen die voor professionele doeleinden aangewend worden en de daarbij horende gebruikersrechten en (audit) log bestanden.

Dit past binnen de opdracht van het bestuur en haar onderstaande doelstellingen:

- 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,
- de bescherming van de belangen van het bestuur,
- de veiligheid en/of de goede technische werking van de netwerkinformaticasystemen, met inbegrip van de controle op de eraan verbonden kosten, alsook de fysieke beveiliging van de installaties van het bestuur,
- de naleving van de principes en gebruiksregels voor het gebruik van online technologieën zoals vermeld in deze richtlijn.

De personeelsleden aanvaarden dat het bestuur het recht heeft controle uit te oefenen op het gebruik van communicatiemiddelen. De controle zal gebeuren op een wijze die de inmenging in de persoonlijke levenssfeer zoveel als mogelijk vermijdt en daar waar het niet anders kan tot een minimum beperkt. Elk personeelslid heeft toegang tot de gegevens met betrekking tot het gebruik van de communicatiegegevens overeenkomstig de bepalingen van de Wet dd. 8 december 1992 en de Algemene Verordening Gegevensbescherming (AVG – van kracht 25 mei 2018) tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.

Mogelijke controles:

- Wat betreft persoonsgegevens neemt het bestuur de nodige technische en organisatorische maatregelen ter beveiliging van deze informatie en heeft de informatieveiligheidsconsulent en/of functionaris gegevensbescherming (DPO) en eventueel ook hogere overheden (wettelijk bepaald) de mogelijkheid om op het

raadplegen, gebruik, verwerking, … van persoonsgegevens controles uit te oefenen en elke personeelslid ter verantwoording te vragen.

- De dienst ICT (o.a. externen die hiertoe aangesteld zijn) mag elke controle uitvoeren die inherent is aan het beheer van de IT-infrastructuur, informatiesystemen en netwerken (*bijvoorbeeld monitoren van het netwerkverkeer op aanvallen van buitenaf, monitoren van e-mail verkeer op verdachte bijlagen die mogelijks een virus kunnen bevatten,…*), om de goede werking ervan te waarborgen of om overbelasting of veiligheidsproblemen te voorkomen of te verhelpen;
- Ook op het gebruik van de andere communicatiemiddelen kan het bestuur eender welke controle uitoefenen.

Dit dient vanzelfsprekend te gebeuren met respect voor de persoonlijke levenssfeer van de personeelsleden en eindgebruikers en met naleving van de toepasselijke wetgeving.

Indien bij deze controles ernstige veiligheidsproblemen, ongeoorloofd gebruik, (*bijvoorbeeld overmatig privégebruik of het moedwillig beschadigen van de goede naam van het bestuur, …*), onregelmatigheden, … worden vastgesteld of indien er ernstige vermoedens ontstaan van misbruik waarbij individualisering van gegevens noodzakelijk is, kan dit gebeuren zonder voorafgaandelijke waarschuwing aan de betrokken gebruiker. Deze controles hebben niet tot doel het individueel gebruik van werknemers na te gaan maar gegevens of communicatie waarvan niet uitdrukkelijk is aangegeven dat het gaat om privé-informatie, kunnen op elk moment door de algemeen directeur of een door hem aangestelde medewerker worden ingekeken.

Indien in het kader van een algemene controle vermoedens zijn ontstaan van het bestaan van inbreuken, kan door het bestuur worden overgegaan tot individualisering, dit wil zeggen dat de communicatiegegevens die tijdens een door de werkgever geïnstalleerde controle werden verzameld worden verwerkt om ze aan een geïdentificeerde of identificeerbare persoon toe te schrijven.

Het personeelslid dat bij toepassing van de procedure van individualisering verantwoordelijk wordt gesteld voor een onregelmatigheid bij het gebruik van de communicatiemiddelen, wordt door het bestuur uitgenodigd voor een gesprek, waarop de verantwoordelijke dagelijks bestuur, de rechtstreeks leidinggevende en de betrokkene zelf aanwezig zijn. Dit gesprek heeft plaats voor iedere beslissing die het personeelslid individueel kan raken. Het gesprek heeft tot doel het personeelslid de kans te bieden zijn bezwaren met betrekking tot de voorgenomen beslissing uiteen te zetten en het gebruik van de hem ter beschikking gestelde communicatiemiddelen te rechtvaardigen.

Indien je van oordeel bent dat je privacy geschonden werd, kan je een klacht indienen bij de Commissie ter bescherming van de Persoonlijke Levenssfeer (Privacy commissie), die terzake een onderzoeksbevoegdheid heeft.

Artikel 9. Sancties

Inbreuken op onderhavig bijlage aan het arbeidsreglement zullen worden gesanctioneerd overeenkomstig de bepalingen van het onderdeel 'sancties en tuchtmaatregelen' van het arbeidsreglement.

Artikel 10. Varia

- Sla je werk heel **regelmatig** op. Beter 1 keer te veel dan dat je bij een eventuele storing opnieuw zou moeten beginnen tenslotte is het maar eventjes op het icoontje "diskette" klikken of via opslaan als.
- De logistiek voor een gemeenschappelijke printer is een eindgebruikers verantwoordelijkheid. De IT-verantwoordelijke is niet bevoegd voor het bijvullen van het papier en de toners.
- Meld onmiddellijk eventuele foutboodschappen op gemeenschappelijke PC's en/of printers aan de IT-verantwoordelijke.